BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-090031
(43)Date of publication of application : 31.03.2000

(51)Int.Cl. G06F 13/00
H04L 12/24
H04L 12/26
H04L 12/56

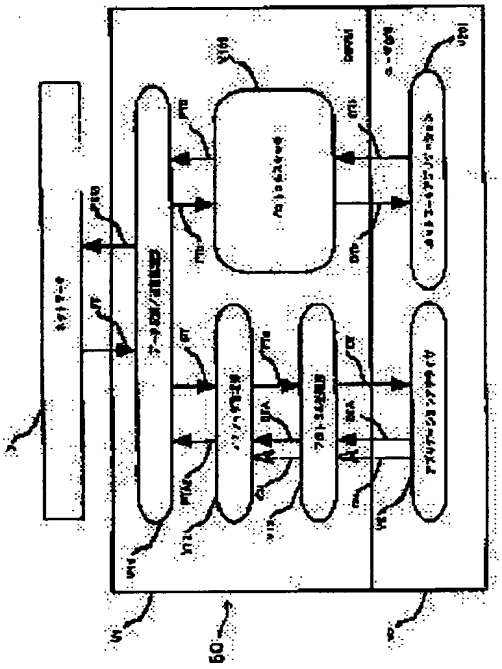
(21)Application number : 10-257363
(22)Date of filing : 11.09.1998

(71)Applicant : ISHII TAKESHI
NATL AEROSPACE LAB
FUJITA NAOYUKI

(72)Inventor : ISHII TAKESHI
FUJITA NAOYUKI

(54) METHOD FOR MONITORING/CONTROLLING NETWORK COMMUNICATION, MONITORING CONTROLLER USING THE SAME AND COMPUTER READABLE RECORDING MEDIUM WHICH RECORDS MONITORING/CONTROLLING PROGRAM OF NETWORK COMMUNICATION

(57)Abstract:
PROBLEM TO BE SOLVED: To easily deal with an arbitrary data system.
SOLUTION: The monitoring/controller of network communication is provided with a data collection/transmission processing part V11 transmitting/receiving packets (PT and PTA1) to/from a network 3, an analyzer managing part V12 provided with a hijack function which executes packet communication with the data collection/transmission processing part V11 based on analyzer managing information rewritten by a control message CM and which individually communicates with communicating persons by the packets (PT and PTA2) when injustice is detected in communication, a protocol processing part V13 reconstituting analysis data DT from the packet PTa and transmitting the control message CM and data DTA and an application analyzer V21 judging whether injustice does not exist in analysis data DT which is taken in and transmitting the control message CM and data DTA in accordance with the judged result.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

先行技術①

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－90031
（P2000－90031A）
(43)公開日　平成12年３月31日(2000.3.31)

(51)Int.Cl.⁷		識別記号	FI			テーマコード（参考）
Ｇ０６Ｆ	13/00	３５３	Ｇ０６Ｆ	13/00	３５３Ｕ	５Ｂ０８９
Ｈ０４Ｌ	12/24		Ｈ０４Ｌ	11/08		５Ｋ０３０
	12/26			11/20	１０２Ｚ	
	12/56					

審査請求　未請求　請求項の数８　ＯＬ　（全 32 頁）

(21)出願番号　特願平10－257363

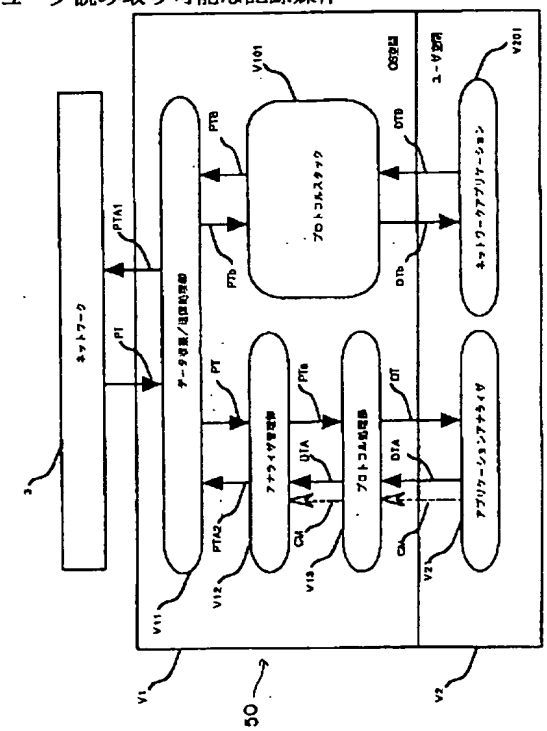
(22)出願日　平成10年９月11日(1998.9.11)

(71)出願人　598124939
石井　剛
東京都調布市染地３－９－51
(71)出願人　391037397
科学技術庁航空宇宙技術研究所長
東京都調布市深大寺東町７丁目44番地１
(71)出願人　597033812
藤田　直行
東京都小金井市前原町４－17－28
(72)発明者　石井　剛
東京都調布市染地３－９－51
(74)代理人　100087468
弁理士　村瀬　一美

最終頁に続く

(54)【発明の名称】　ネットワーク通信の監視・制御方法及びこれを利用した監視・制御装置並びにネットワーク通信の監視・制御プログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　任意のデータ形式を簡便に取り扱う。
【解決手段】　ネットワーク通信の監視・制御装置は、ネットワーク３に対してパケット（PT，PTA1）を送受信できるデータ収集／送信処理部V11 と、制御メッセージCMによって書き換えられるアナライザ管理情報を基にデータ収集／送信処理部V11 との間でパケット通信を行い、通信に不正を検知したときパケット（PT，PTA2）でもって通信当事者と個々に通信するハイジャック機能を備えたアナライザ管理部V12 と、パケットPTa から解析データDTを再構築し、制御メッセージCM及びデータDTAを送出するプロトコル処理部V13 と、取り込んだ解析データDTに不正がないか判断し、その判断結果に応じて制御メッセージCM及びデータDTAを送出するアプリケーションアナライザV21 とを備える。



【特許請求の範囲】

【請求項１】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、前記ネットワークに対してパケットを送受信できるデータ収集／送信処理工程と、制御メッセージによって書き換えられるアナライザ管理情報を基に前記データ収集／送信処理工程との間でパケット通信を行うとともに、通信に不正が検知されたときには前記パケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理工程と、前記アナライザ管理工程から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータを前記アナライザ管理工程に伝送するプロトコル処理工程と、前記プロトコル処理工程から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理工程に送出するアナライザ工程とを備えたことを特徴とするネットワーク通信の監視・制御方法。

【請求項２】　前記データ収集／送信処理工程からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにして前記データ収集／送信処理工程に与えるデータ作成送出工程と、前記データ作成送出工程から解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データを前記データ作成送出工程に与えるネットワーク処理工程とを備えたことを特徴とする請求項１に記載のネットワーク通信の監視・制御方法。

【請求項３】　前記データ収集／送信処理工程、アナライザ管理工程、プロトコル処理工程及びデータ作成送出工程、または前記データ収集／送信処理工程及びデータ作成送出工程がオペレーティングシステム空間に実装されたものであることを特徴とする請求項１または２記載のネットワーク通信の監視・制御方法。

【請求項４】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する装置であって、前記ネットワークに対してパケットを送受信できるデータ収集／送信処理部と、制御メッセージによって書き換えられるアナライザ管理情報を基に前記データ収集／送信処理部との間でパケット通信を行うとともに、通信に不正が検知されたときには前記パケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理部と、前記アナライザ管理部から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータを前記アナライザ管理部に伝送するプロトコル処理部と、前記プロトコル処理部から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理部に送出するアプリケーションアナライザとを備えたことを特徴とするネットワーク通信の監視・制御装置。

【請求項５】　前記データ収集／送信処理部からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにして前記データ収集／送信処理部に与えるプロトコルスタックと、前記プロトコルスタックから解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データを前記プロトコルスタックに与えるネットワークアプリケーションとを備えたことを特徴とする請求項４に記載のネットワーク通信の監視・制御装置。

【請求項６】　前記データ収集／送信処理部、アナライザ管理部、プロトコル処理部及びプロトコルスタック、または前記データ収集／送信処理部及びプロトコルスタックがオペレーティングシステム管理空間に実装されたものであることを特徴とする請求項４または５記載のネットワーク通信の監視・制御装置。

【請求項７】　情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、前記ネットワークに対してパケットを送受信できるデータ収集／送信処理手順と、制御メッセージによって書き換えられるアナライザ管理情報を基に前記データ収集／送信処理手順との間でパケット通信を行うとともに、通信に不正が検知されたときには前記パケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理手順と、前記アナライザ管理手順から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータを前記アナライザ管理手順に伝送するプロトコル処理手順と、前記プロトコル処理手順から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理手順に送出するアナライザ手順とをコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記憶媒体。

【請求項８】　前記データ収集／送信処理手順からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにして前記データ収集／送信処理手順に与えるデータ作成送出手順と、前記データ作成送出手順から解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データを前記データ作成送出手順に与えるネットワーク処理手順とをコンピュータに実行させるためのプログラムを記録した請求項７記載のコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ネットワーク通信の監視・制御方法及びこれを利用した監視・制御装置並

びにネットワーク通信の監視・制御プログラムを記録したコンピュータ読み取り可能な記録媒体に関する。

【０００２】さらに詳述すると、本発明は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおいて、通信されるデータに不正が発生しているか否かを解析し、ネットワークのセキュリティやネットワーク管理を実行できるとともに、情報通信ステーションのオペレーティングシステムへのインターフェースとして実現されているネットワーク通信の監視・制御方法及びこれを利用した監視・制御装置並びにネットワーク通信の監視・制御プログラムを記録したコンピュータ読み取り可能な記録媒体に関するものである。

【０００３】なお、本発明において、ネットワークにおける「不正」とは、例えばクラッキング等のいわゆる不正アクセスを意味する。

【０００４】

【従来の技術】従来、情報通信ステーションの間で通信を行うように構築されたネットワークにおいて、その通信データに不正が発生しているか否かを監視する監視ツールが提供されている。

【０００５】かかる従来のネットワーク監視ツールとしては、大別して、「パケット単位の監視ツール」と、「代理サーバ形式の監視ツール」とが挙げられる。

【０００６】図３８に、従来のパケット単位の監視ツールの構成例を示す。このパケット単位の監視ツールは、図３８に示すように、ネットワークＮＴＷで接続された通信装置ＭＣＮＡ、ＭＣＮＢの間に通信装置ＭＣＮＣを備え、この通信装置ＭＣＮＣの内部で実現されるものである（第１の従来技術）。各通信装置ＭＣＮＡ、ＭＣＮＢは、当該装置内のオペレーティングシステム（ＯＳ）空間にプロトコルスタックを、同ユーザ空間に通信ライブラリ及びアプリケーションを備えている。また、通信装置ＭＣＮＣは、当該装置内のＯＳ空間にプロトコルスタックを、同ユーザ空間に通信ライブラリ及び従来のアナライザを備えている。

【０００７】このような両通信装置ＭＣＮＡ、ＭＣＮＢの間で通信を行っている場合に、ネットワークＮＴＷ上を流れるパケット（通信内容[Hello B!]、通信相手[A->B]）ＰＴを通信装置ＭＣＮＣがそのまま受け取り、各種プロトコルを通信装置ＭＣＮＣで実現したツール（従来のアナライザ）自らの責任で監視するものである。この種類のツールは作成が容易で数多く開発されている（Sniffer,Real Secure,NetRanger）。

【０００８】図３９に、従来の代理サーバ形式の監視ツールの構成例を示す。この代理サーバ形式の監視ツールは、図３９に示すように、ネットワークＮＴＷで接続された通信装置ＭＣＮＡ、ＭＣＮＢの間に通信装置ＭＣＮＣを備え、この通信装置ＭＣＮＣが実際のサービスを中継することによって通信内容を傍受し解析することにより実現されるものである（第２の従来技術）。両通信装置ＭＣＮＡ、ＭＣＮＢは、当該装置内のＯＳ空間にプロトコルスタックを、同ユーザ空間に通信ライブラリ及びアプリケーションを備えている。また、通信装置ＭＣＮＣは、当該装置内のＯＳ空間にプロトコルスタックを、同ユーザ空間に通信ライブラリ及び代理サーバを備えている。

【０００９】このような両通信装置ＭＣＮＡ、ＭＣＮＢの間で通信を行っている場合に、例えば通信装置ＭＣＮＡはネットワークＮＴＷ上にパケット（通信内容[Hello B!]、通信相手[A->C]）ＰＴを送出する。すると、通信装置ＭＣＮＣは、ウィルススキャナのように、プロトコルスタック及び通信ライブラリを介して当該パケットＰＴから通信内容[Hello B!]を受け取って当該通信内容を代理サーバが傍受し解析し、問題なければ、再び、当該通信内容を通信ライブラリ及びプロトコルスタックに渡して、この通信内容に通信相手[C->B]を付加してネットワークＮＴＷを介して通信装置ＭＣＮＢに渡すようにしたものである。この監視ツールによれば、ＴＣＰのようなコネクション指向の通信を正確に監視できるという利点がある(ServerProtect,VirusBuster)。

【００１０】

【発明が解決しようとする課題】しかしながら、上記第１の従来技術によれば、ツール自体が多くのプロトコルを処理する基本設計になっているためツール自体が巨大化すること、パケット単位のデータをツール自体の責任で処理するためユーザが新しいものを作り出すのが難しいこと、等の欠点があった。

【００１１】また、この第１の従来技術によれば、ＴＣＰ（Transport Control Protocol）のようなコネクション指向のプロトコルを処理するには、ツールの中でマルチタスク化等を行う必要があり、ユーザに高度なプログラミング技術を要求することになる。このため、多くの場合、この種のツールはパケット単位の監視のみを行うこととなり、セッション単位の監視を行うことができないという欠点があった。

【００１２】また、上記第２の従来技術によれば、サーバ及びクライアントの環境が代理サーバの存在を前提に構築されている必要があること、パケット単位の監視は不可能であること、などの問題点がある。

【００１３】そこで、本発明の第１の目的は、アプリケーションのセッションを含め任意のデータ形式を簡便に取り扱うネットワーク通信の監視・制御方法及びこれを利用した監視・制御装置並びにネットワーク通信の監視・制御プログラムを記録したコンピュータ読み取り可能な記録媒体を提供することにある。

【００１４】また、本発明の第２の目的は、データの単位を限定することなく、かつ、ネットワーク通信における既存機器に変更を加えることなく、簡便にネットワークの監視・制御を行う方法及び装置並びにその制御プロ

グラムを記憶した記憶媒体を提供することにある。

【００１５】さらに、本発明の第３の目的は、簡便に利用できるユーザインターフェースをを提供することにある。

【００１６】

【課題を解決するための手段】本発明者らは、従来の監視ツールについて検討した結果、オペレーティングシステムがネットワークの監視・制御ツールの存在を予期することなく設計されたことが上記欠点や問題点を招来させた原因であること、ネットワーク通信がオペレーティングシステムに組み込まれた機能を利用することを前提としており、オペレーティングシステムのサポートなしで当該ツールを開発するのは困難かつ非効率的なことであることを見い出し、これを次のようにすることによって解決した。

【００１７】すなわち、多くのネットワーク通信の中からある特定のネットワーク通信を選択するためには、

(i) 発信者の識別子群

(ii)受信者の識別子群

(iii) 通信のトリガ

を指定する必要がある。

【００１８】しかしながら、現在のプロトコルスタックと通信ライブラリには、後述する制限が存在するため、この３種類の条件を全てを指定することはできない。以下には、その制限とこれを解決するための手段を挙げる。

【００１９】第１に、プロトコルスタックと通信ライブラリに施す変更点について検討する。

【００２０】＜プロトコルスタックに対する変更点＞プロトコルスタックは通常階層構造になっている。ネットワークの物理的な処理を行う層からアプリケーションに近い層まで、多くのプロトコル層が存在する。また、プロトコルスタックは通常同時に複数の通信を処理する。その際、ある通信と別の通信を区別する識別子が必要となる。各プロトコル層で通信のなんらかの識別子を１つまたは複数持つことが多く、その個別の識別子をID(m)と書き、識別子候補と呼ぶことにする。通信はサーバとクライアントの組みで行われるので、サーバ側の識別子候補をSID(m)、クライアント側の識別子候補をCID(m)と書くことにする。１つの通信はSID(m)とCID(m)の組みで表すことができる。これを通信の識別子と呼びＩと書くことにする。

【００２１】ここで、サーバ側のプロトコルスタックに注目すると、通信の識別子Ｉは数式１のように記述できる。

【００２２】

【数１】S = (SID(0), ..., SID(s))

C = (CID(0), ..., CID(c))

但し（すべてのmについて）(SID(m) はサーバのアドレスを表さない)。

【００２３】この条件のもとで、数式２のようになる。

【００２４】

【数２】I = S∧C

そして、SID(m)の中でサーバ自身を表すアドレスのような値は除外される。なぜなら、サーバ自身が通信しているということは自明であるからである。クライアントのプロトコルスタックも同様に数式３のように表される。

【００２５】

【数３】S = (SID(0), ..., SID(s))

C = (CID(0), ..., CID(c))

但し（すべてのmについて）(CID(m) はクライアントのアドレスを表さない)

I = S∧C

【００２６】さて、ネットワーク解析ツールのためのプロトコルスタックを考えた場合、プロトコルスタックを実装しているホストが通信の当事者であるという前提を取り除かなければならない。すると通信識別子I'を数式４のように表すことができる。

【００２７】

【数４】

S' = (SID(0), ..., SID(s))

C' = (CID(0), ..., CID(c))

但し（あるmについて）(SID(m) はサーバのアドレスを表す)

（あるmについて）(CID(m)はクライアントのアドレスを表す)

さらに、このような条件のもとで、数式５のように表現することができる。

【００２８】

【数５】I' = S' ∧ C'

【００２９】＜通信ライブラリに対する変更点＞従来の通信ライブラリは必ず通信の当事者用に設計されていた。サーバであるならば、サーバとして行うサービスアドレスの指定、クライアントであるならば、サーバのアドレス等を指定できるよう通信ライブラリが作られている。

【００３０】すなわち、func(アドレス指定)　ここで、アドレスはサーバまたはクライアントを特定するものである。

【００３１】クライアントがサーバにアクセスするタイミングを持って通信開始とする。つまり、そのタイミングをトリガとして扱っている。

【００３２】ここで、ネットワーク監視ツールのためのライブラリはどのような変更が必要になるかを考えると、ネットワーク監視ツールは通信の非当事者のため通信開始というタイミングがない。そこで、監視対象の通信が開始された時点をもってネットワーク監視ツールもアクティブになればよい。

【００３３】しかしながら、もっと一般的にネットワーク通信を表すなんらかのトリガがありさえすればよい。

通信の非当事者のため必ずしも通信開始をトリガにする必要はない。言い換えれば、従来のアドレス指定は、下記のようにトリガ指定の中に含まれて記述できるようになる。

【００３４】func(トリガ指定)

例えばトリガとしては次のようなものである。

【００３５】・CID(0)=123 かつSID(5)=456の通信

・SID(0)=1かつSID(1)=2かつSID(3)=3の通信

・全ての通信

【００３６】第２に不正な通信に対する制御方法について検討する。これは、不正な通信が行われているときに、単に、不正が存在するとするだけでなく、この不正に積極的に関与して不正な通信がされないようにするものである。以下、その不正な通信をさせない一つの対策である「通信のハイジャック機能」について検討する。

【００３７】＜通信のハイジャックについて＞ネットワーク通信は通常サーバとクライアントの間で行われる。通信経路の途中でその通信を切断し、切断者がサーバとクライアントとのそれぞれと通信を行う。サーバはクライアントと、クライアントはサーバと通信しているつもりであるが、これらの実際の通信相手は切断者である。これを通信のハイジャックと呼ぶことにする。従来から通信のハイジャックは行われてきた。しかしながら、それは、一時的にまたは数パケットのみのハイジャックであったり、あるいは通信のタイミングに厳密性が必要であって多くの試行をくり返した後ハイジャックに成功するというようなものであった。

【００３８】すなわち、このような従来のハイジャック技術では、ネットワーク侵入者に対して、攻撃的な対応をとることは不可能であり、通信の不正の発覚時に管理者が通信を切断するというあくまで防御の手段しか取りえなかった。

【００３９】本発明において実現する通信のハイジャック機能は侵入者に対して初めて攻撃的な対応を管理者に与えるものである。

【００４０】＜ハイジャックのために必要な変更＞通信の非当事者用のプロトコルスタックと通信ライブラリをデュアルホームホストに適用すると、通信のハイジャックが可能になる。以下、具体的な変更点について説明する。

【００４１】＜プロトコルスタックに対する変更＞プロトコルスタックに対する変更については、以下のようなものがある。

【００４２】・２インターフェース対応

・パケットのフォワード

・パケットのフォワード禁止ルール

・アプリケーションからの要求によるパケットの作成

【００４３】＜通信ライブラリに対する追加＞通信ライブラリに対して追加する項目は、ハイジャックを行うための関数及びハイジャック後の通信を行うための関数とが挙げられる。

【００４４】デュアルホームホストの片方に実際の通信のサーバ、他方に実際の通信のクライアントがあるとし、デュアルホームホストにてパケットのフォワードを行っている場合を想定する。さらに、このホスト上でネットワーク解析ツールがサーバとクライアントの通信を解析しているとする。このときネットワーク解析ツールはサーバとクライアントの通信遮断を要求することができる（通信ライブラリに対する追加機能による）。デュアルホームホストのプロトコルスタックはパケットフォワード禁止ルールに要求のあった通信を登録する。この時点でサーバとクライアントの通信は切断される。次にネットワーク解析ツールはサーバと対話することができる（プロトコルスタックのパケット作成機能による）。

【００４５】サーバは依然としてクライアントと通信を続けているようで、実はネットワーク解析ツールと対話をしているのである。クライアントに対しても同様である。

【００４６】上述した検討に基づいて想起された請求項１記載の発明に係るネットワーク通信の監視・制御方法は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、ネットワークに対してパケットを送受信できるデータ収集／送信処理工程と、制御メッセージによって書き換えられるアナライザ管理情報を基にデータ収集／送信処理工程との間でパケット通信を行うとともに、通信に不正が検知されたときにはパケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理工程と、アナライザ管理工程から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータをアナライザ管理工程に伝送するプロトコル処理工程と、プロトコル処理工程から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理工程に送出するアナライザ工程とを備えたことを特徴とする。

【００４７】したがって、パケットから解析データを再構築して解析できるので、再構築後のデータにより不正の判断を行うことができる。また、デュアルホームホストの採用によりハイジャック機能を実現できるので、ネットワークでの不正を防止することができる。

【００４８】また、請求項２記載の発明は、請求項１において、データ収集／送信処理工程からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにしてデータ収集／送信処理工程に与えるデータ作成送出工程と、データ作成送出工程から解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データをデータ作成送出工程に与えるネットワーク処理工程とを備えたことを特徴

とする。

【００４９】さらに、請求項３記載の発明は、請求項１または２において、データ収集／送信処理工程、アナライザ管理工程、プロトコル処理工程及びデータ作成送出工程、またはデータ収集／送信処理工程及びデータ作成送出工程がオペレーティングシステム空間に実装されたものであることを特徴とする。

【００５０】したがって、ユーザ空間にアプリケーションとして実装する場合に比べて優先的に実行されると共にメモリ等の使用頻度が非常に少なくなるので、処理速度を格段に向上させることができる。

【００５１】上記目的を達成するために、請求項４記載の発明に係るネットワーク通信の監視・制御装置は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する装置であって、ネットワークに対してパケットを送受信できるデータ収集／送信処理部と、制御メッセージによって書き換えられるアナライザ管理情報を基にデータ収集／送信処理部との間でパケット通信を行うとともに、通信に不正が検知されたときにはパケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理部と、アナライザ管理部から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータをアナライザ管理部に伝送するプロトコル処理部と、プロトコル処理部から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理部に送出するアプリケーションアナライザとを備えたことを特徴とする。

【００５２】したがって、パケットから解析データを再構築して解析できるので、再構築後のデータにより不正の判断を行うことができる。また、デュアルホームホストの採用によりハイジャック機能を実現できるので、ネットワークでの不正を防止することができる。

【００５３】請求項５記載の発明は、請求項４において、データ収集／送信処理部からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにしてデータ収集／送信処理部に与えるプロトコルスタックと、プロトコルスタックから解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データをプロトコルスタックに与えるネットワークアプリケーションとを備えたことを特徴とする。

【００５４】請求項６記載の発明は、請求項４または５において、データ収集／送信処理部、アナライザ管理部、プロトコル処理部及びプロトコルスタック、ないし、データ収集／送信処理部及びプロトコルスタックがオペレーティングシステム管理空間に実装されたものであることを特徴とする。

【００５５】したがって、ユーザ空間にアプリケーションとして実装する場合に比べて優先的に実行されると共にメモリ等の使用頻度が非常に少なくなるので、処理速度を格段に向上させることができる。

【００５６】請求項７記載の発明に係るコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記憶媒体は、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析する方法であって、ネットワークに対してパケットを送受信できるデータ収集／送信処理手順と、制御メッセージによって書き換えられるアナライザ管理情報を基にデータ収集／送信処理手順との間でパケット通信を行うとともに、通信に不正が検知されたときにはパケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理手順と、アナライザ管理手順から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータをアナライザ管理手順に伝送するプロトコル処理手順と、プロトコル処理手順から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理手順に送出するアナライザ手順とをコンピュータに実行させるためのプログラムを記録している。

【００５７】したがって、コンピュータで記録媒体に格納されたプログラムを読み取り、インストールすることによって、あるいはそのままプログラムを実行することによって、ネットワーク伝送時にデータ部分に発生した不正を容易に判別することができる。

【００５８】請求項８の発明は、請求項７において、データ収集／送信処理手順からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにしてデータ収集／送信処理手順に与えるデータ作成送出手順と、データ作成送出手順から解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データをデータ作成送出手順に与えるネットワーク処理手順とをコンピュータに実行させるためのプログラムを記録した記憶媒体である。

【００５９】

【発明の実施の形態】以下、本発明の構成を図面に示す実施の形態に基づいて詳細に説明する。

【００６０】〔第１の実施の形態〕図２に、本発明に係るネットワーク不正解析方法が適用されたネットワークシステムの一例を示す。

【００６１】この図２において、符号１は構内ネットワーク（以下、「ＬＡＮ」という）であり、このＬＡＮ１にはルータ２を介して緩衝帯ネットワーク３が接続されている。この緩衝帯ネットワーク３は、ルータ６を介して外部ネットワーク７に接続されている。

【００６２】本実施形態ではＬＡＮ１は、複数のステー

ション（図示せず）と、これらステーションを結ぶネットワーク（図示せず）と、外部に接続する外部接続回線１１とからなる。この外部接続回線１１はルータ２に接続されている。但し、ＬＡＮ１としては上述のものに限られず、単一のステーションから成るものとすることもできる。

【００６３】緩衝帯ネットワーク３は、本発明に係るネットワーク不正解析方法を実現するネットワーク不正解析システム５０と、コモンバス５１と、外部接続回線５２、５３とからなる。ネットワーク不正解析システム５０はコモンバス５１に接続されている。外部接続回線５２はルータ２とコモンバス５１とを接続している。外部接続回線５３はコモンバス５１とルータ６とを接続している。

【００６４】また、ネットワーク不正解析システム５０は従来のネットワーク不正解析システムと同様にコンピュータシステムにて構成される。このコンピュータシステムは、特に図示していないが、例えば各種の演算処理を実行する中央演算処理装置と、演算処理を実行する上で必要なプログラムやデータ等を記憶する主記憶装置と、入出力ポート等の各種インタフェースと、このネットワーク不正解析システムを実現するプログラムやその処理を実行する上で必要な各種データや定数等を記憶する例えばハードディスクドライブ装置と、データや必要な指令を入力する入力装置と、中央演算処理装置で処理した結果を出力する出力装置とから構成されるのが一般的である。

【００６５】図３に、本発明に係るネットワーク不正解析方法の実施の一形態を示す。この図３において、ネットワーク不正解析システム５０は、中央演算処理装置が主記憶装置に記憶されたプログラムを処理することにより実現されるものであって、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するシステムである。すなわち、ネットワーク不正解析システム５０は、例えば緩衝帯ネットワーク３で伝送されているパケットＰＴを取り込むデータ収集工程を実行するデータ収集部５５と、データ収集部５５からのパケットＰＴａを各階層化モジュールでフィルタリング及び再構築することにより解析データＤＴを作成するデータ作成工程を実行するデータ作成部５６と、データ作成部５６からの解析データＤＴに不正が発生しているか判定して解析結果ＣＤＣを出力するデータ解析工程を実行するデータ解析部５７とから構成されている。

【００６６】図１に、ネットワーク不正解析システム５０の詳細構成を示す。この図１において、データ収集部５５は、例えば緩衝帯ネットワーク３の間で伝送されているパケットＰＴを取り込むデータ収集処理部５５１と、このデータ収集処理部５５１のデータ収集処理を制御するデータ収集制御部５５２とから構成されている。データ収集処理部５５１は、収集したパケットＰＴをデータ作成部５６に供給する。

【００６７】データ作成部５６は、階層化されたプロトコルに応じた階層化モジュールのパラメータを、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集部５５からのパケットＰＴａを各階層化モジュールでフィルタリングしてパケットＰＴａの細分化されたデータを元の単位に再構築することにより解析データＤＴを作成するデータ作成工程を実行するものである。

【００６８】このデータ作成部５６は、大別すると、階層化モジュール５６１と、これを制御し管理する制御管理部５６２とから構成されている。制御管理部５６２は、予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて、階層化されたプロトコルに応じた階層化モジュール５６１のパラメータを設定できる。また、階層化モジュール５６１は、設定に基づいてデータ収集部５５からのパケットＰＴａをフィルタリングしてパケットＰＴａの細分化されたデータを元の単位に再構築することにより解析データＤＴを作成できるようになっている。

【００６９】階層化モジュール５６１は、１レイヤモジュール61_1，…，ｋレイヤモジュール61_k，…，Ｎレイヤモジュール61_Nからなる複数のレイヤモジュールから構成されている。ここで、Ｎは任意の整数であり、ｋは１～Ｎの間の任意の整数である。

【００７０】１レイヤモジュール61_1は、読み込まれたコンフィグレーションファイルの内容に応じて、１レイヤフィルタ61_{1A}および１レイヤ再構築部61_{1B}が構成される。ｋレイヤモジュール61_kは、読み込まれたコンフィグレーションファイルの内容に応じて、ｋレイヤフィルタ61_{kA}およびｋレイヤ再構築部61_{kB}が構成される。Ｎレイヤモジュール61_Nは、読み込まれたコンフィグレーションファイルの内容に応じて、Ｎレイヤフィルタ61_{NA}およびＮレイヤ再構築部61_{NB}が構成される。そして、各レイヤモジュール61_1，…，61_k，…，61_Nは、１からＮまで順に処理される。

【００７１】制御管理部５６２は、各レイヤモジュール61_1，…，61_k，…，61_Nにおいてデータを作成するデータ作成制御部６２ａと、各レイヤモジュール61_1，…，61_k，…，61_Nにおいてデータの記憶を制御するメモリ制御部６２ｂと、解析データＤＴを出力させるためのアナライザ管理部６２ｃとから構成されている。そして、制御管理部５６２は、１レイヤモジュール61_1，…，ｋレイヤモジュール61_k，…，Ｎレイヤモジュール61_Nをそれぞれ制御及び管理する。

【００７２】データ解析部５７は、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部５６からの解析データＤＴに不正が発生しているか判定して解析結果ＣＤＣを出力するデータ解

析工程を実行するものである。

【００７３】このデータ解析部５７には、アプリケーション層セッション単位のデータに不正が有るかを解析するアプリケーションアナライザ５７０が設けられている。そして、このアプリケーションアナライザ５７０は、予め読み込んだコンフィグレーションファイルに記載されている内容に基づいてフィルタリング及び再構築されたデータＤＴに不正がないか否かを解析する。

【００７４】図４に、コンフィグレーションファイルの例を示す。この図４において、コンフィグレーションファイル５００は、データ作成部５６からデータ解析部５７に渡すデータＤＴの指定をするための情報やデータ解析部５７で解析する情報を書き込むことができるようになっており、例えば図４に示すような内容を記載できるようになっている。

【００７５】図５に、解放型システム間相互接続（ＯＳＩ；Open System Interconnection）の７層モデルの例を示す。この図に示す階層化モデル８００は、解放型システムの通信機能を７つに階層化したものであり、物理レイヤ８０１、データリンクレイヤ８０２、ネットワークレイヤ８０３、トランスポートレイヤ８０４、セッションレイヤ８０５、プレゼンテーションレイヤ８０６、アプリケーションレイヤ８０７に階層化されている。

【００７６】物理レイヤ８０１は、ビット伝送に必要な物理的条件や電気的条件が定められている。データリンクレイヤ８０２は、データ伝送誤り制御手順等が定められている。ネットワークレイヤ８０３は、公衆パケット交換等各種通信網を介して両端のシステム間でデータのやりとりを可能とするためのものである。トランスポートレイヤ８０４は、両端のシステムの間で透過的で信頼性の高いデータ転送を行うためのものである。セッションレイヤ８０５は、両端のアプリケーションプロセスでの対話を効率よく行うため、同期をとったり伝送モードの選択、送信権の制御を行うためのものである。プレゼンテーションレイヤ８０６は、両端のアプリケーションプロセスが扱うデータを正確にかつ効率よく転送できるようにデータ形式を制御するためのものである。アプリケーションレイヤ８０７は、ユーザが実行する様々なアプリケーションに応じて、ファイル転送、メッセージ通信処理システム、下層端末、遠隔データベースアクセスなどのアプリケーションサービス要求を実行するためのものである。

【００７７】このように構成されたネットワーク不正解析システム５０の動作を図６～図８に説明する。図６に、同システム５０の動作を説明するためのフローチャートを示す。図７，８に、同システムによって処理されるデータの内容の例を示す。

【００７８】ここで、緩衝帯ネットワーク３のコモンバス５１上を一つの意味有る情報ないしデータを構築する複数のデータパケット、例えば通信データ９０ａ，９０ｂ，９０ｃ，９０ｄが流れているとする。

【００７９】これらの通信データ９０ａ，９０ｂ，９０ｃ，９０ｄは、例えば図７に示すように受信先ＩＤ９１ａ，９１ｂ，９１ｃ，９１ｄと、送信元ＩＤ９２ａ，９２ｂ，９２ｃ，９２ｄと、順番９３ａ，９３ｂ，９３ｃ，９３ｄと、データ９４ａ，９４ｂ，９４ｃ，９４ｄとから構成されている。

【００８０】このコモンバス５１上の伝送される通信データ９０ａは、次のようにして構成されている。すなわち、例えば「I am a cracker.」というアプリケーションレイヤでのデータ９５は細分化されて（ステップ（Ｓ２１）、「I am」というデータ９４ｂと、「ac」というデータ９４ｄと、「rac」というデータ９４ａと、「ker.」というデータ９４ｃとに分割されたデータとなる。そして、さらに細分化されて（Ｓ２２）、ヘッダを付けた通信データ９０ａ，９０ｂ，９０ｃ，９０ｄにされ、これらは図５に示す階層化モデル８００によりネットワーク上を伝送されることになる。緩衝帯ネットワーク３上でのデータ単位は、通信データ９０ａ，９０ｂ，９０ｃ，９０ｄとなる。このデータ単位で、緩衝帯ネットワーク３のコモンバス５１上を伝送されることになる。

【００８１】図６に示すように、ネットワーク不正解析システム５０は、コンフィグレーションファイルを読み込む（Ｓ１１）。これにより、データ作成部５６の１レイヤモジュール61_1の１レイヤフィルタ61_{1A}及び１レイヤ再構築部61_{1B}，…，ｋレイヤモジュール61_kのｋレイヤフィルタ61_{kA}及びｋレイヤ再構築部61_{kB}，…，Ｎレイヤモジュール61_NのＮレイヤフィルタ61_{NA}及びＮレイヤ再構築部61_{NB}には、データ解析部５７に渡すデータやフィルタリング及び再構築すべきデータに関するパラメータが設定される。また、このコンフィグレーションファイルにより、データ解析部５７で解析する内容が設定される。

【００８２】ここで、Ｎの値は、図５に示す階層化モデル８００のどの階層までのデータとして再構築するかにより決定される。本実施形態では、Ｎ＝７としてアプリケーション層セッション単位にまで再構築している。但し、Ｎ＝７に限られず、例えばＮ＝３としてネットワーク層セッション単位にまで再構築するようにもできる。いずれの場合もデータ解析に必要なセッション単位にまで再構築するように設定できる。

【００８３】次に、データ収集部５５は、データ収集制御部５５２の制御下に、コモンバス５１の上を伝送されているパケットＰＴの１パケット（例えば通信データ９０ａ）を取り込み（Ｓ１２）、この１パケットがコンピュータシステムの主記憶装置またはハードディスクドライブ装置等にある作業エリアにコピーされる（Ｓ１３）。これにより、この作業エリアにコピーされた１パケットは、階層化モジュール５６１の１レイヤモジュー

ル６１$_1$に取り込まれ、コンフィグレーションファイルの情報に応じて１レイヤ目の処理を実行して次の層のレイヤモジュールに渡す（Ｓ１４）。この１レイヤモジュール６１$_1$では、パケットのヘッダ部のさまざまなフィールドの中の値と、コンフィグレーションファイルで指定されたフィルタ通過パラメータとの比較を行い、コンフィグレーションファイルで指定されているデータを選びだす処理を実行したり、通過処理したりする。また、フィルタ通過処理ではデータを変更しない。

【００８４】次いで、１レイヤモジュール６１$_1$の下層の各レイヤモジュールは、上述と同様にコンフィグレーションファイルの内容に応じてそれぞれ処理を実行する。

【００８５】ｋレイヤモジュール６１$_k$の前のモジュールが処理した結果をｋレイヤモジュール６１$_k$が受け取る。

【００８６】ここで、各レイヤモジュール６１$_1$，…，６１$_k$，…，６１$_N$では同様の処理が実行されるので、一例としてｋレイヤモジュール６１$_k$について詳細に説明する。

【００８７】ｋレイヤモジュール６１$_k$は、予め読み込まれたコンフィグレーションファイルの情報に応じて、受け取ったデータをｋレイヤフィルタ６１$_{kA}$に通すのか否か、ｋレイヤ再構築部６１$_{kB}$を動作させるのか否か、あるいは再構築あるいは非再構築のデータをデータ解析部５７に渡すか否かのパラメータが設定されているので、そのパラメータの設定に従って処理を実行する（Ｓ１５）。

【００８８】例えば、コンフィグレーションファイルの情報の指定によって各パラメータが設定されているとすると、ｋレイヤモジュール６１$_k$では、上層のレイヤモジュールが処理した結果のデータをｋレイヤフィルタ６１$_{kA}$を通過させたのち（Ｓ１５１；ＹＥＳ）、そのデータを再構築する場合には（Ｓ１５２；ＹＥＳ）、バッファを使用して再構築し（Ｓ１５３）、アプリケーション層単位でのデータにまでの再構築が完了しない場合には（Ｓ１５４；ＮＯ）、ｋレイヤモジュール６１$_k$を抜ける。そして、次のパケットを読み込む（Ｓ１２）。

【００８９】また、バッファを使用して再構築し（Ｓ１５３）、再構築が完了した場合（Ｓ１５４；ＹＥＳ）にはｋレイヤ再構築部６１$_{kB}$のバッファにデータが蓄えてられている。この場合あるいはデータを再構築しない場合（Ｓ１５２；ＮＯ）には、再構築したデータをデータ解析部５７に渡すタイミイグになったときに（Ｓ１５５；ＹＥＳ）、ｋレイヤ再構築部６１$_{kB}$のバッファに蓄えていたデータをデータ解析部５７に渡す（Ｓ１５６）。また、データ解析部５７に渡さないタイミングになったところで（Ｓ１５５；ＮＯ）、これより上側の層のレイヤモジュールにデータを渡す。

【００９０】これにより、ｋレイヤモジュール６１$_k$より上層のレイヤモジュールで処理された結果、図８に示すように再構築されて（Ｓ２３）、分割されたデータとして「rac 」というデータ９４ａがデータ解析部５７に渡る。

【００９１】以上の処理を１パケット毎に繰り返すことにより（Ｓ１３～Ｓ１６）、ネットワーク上でのデータ単位のパケットＰＴは、図８に示すように再構築され（Ｓ２３）、「I am」というデータ９４ｂと、「ａｃ」というデータ９４ｄと、「rac」というデータ９４ａと、「ker.」というデータ９４ｃとに分割されたデータとなる。さらに、再構築されて（Ｓ２４）、「I am a cracker. 」というアプリケーションレイヤでの元のデータ９５にされる。

【００９２】下位の層のレイヤモジュールが上記のようにコンフィグレーションファイルの情報によって各パラメータが設定されているとすると、Ｎレイヤフィルタ６１$_N$にまでデータが渡る。

【００９３】Ｎレイヤフィルタ６１$_N$では、上述と同様にコンフィグレーションファイルの情報により設定されたパラメータで受け取ったデータの処理を行い、解析データＤＴとしてデータ解析部５７に渡す（Ｓ１６）。

【００９４】また、このフローチャートを使用すれば、複数の種類のフィルタを設定することにより複数の種類のクラッキング等の不正アクセスを同時に監視できる。

【００９５】データ解析部５７では、アプリケーションアナライザ５７０が予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成部５６からの解析データＤＴに不正が発生しているか判定している。このアプリケーションアナライザ５７０の判定した結果は、例えばディスプレイ上に、図９に示すような画面９００として表示される。

【００９６】ここで、アプリケーションアナライザ５７０は、不正解析処理を次のいずれか一方あるいは双方を採用するようにしている。但し、これらの処理方法に限られないのは勿論である。

【００９７】（ｉ）注目しているプロトコルでどのような操作をすれば、不正が実行可能かを調べておき、その手順をアプリケーションアナライザ５７０用のコンフィグレーションファイルに記述しておき、解析データＤＴとコンフィグレーションファイルに記載された手順を比較して一致すれば、その通信は不正なものであると判断処理を実行する。

【００９８】（ii）セキュリティを確保するために厳重に管理する必要があるファイルやプログラム等をアプリケーションアナライザ５７０用のコンフィグレーションファイルに記載しておき、記載しておいたリソースに変化があった時点で、その通信は不正なものであると判断処理を実行する。

【００９９】上述したネットワーク不正解析システム５０によれば、例えば次のような不正（クラッキング）を

防止できる。

【０１００】（１）ＴＣＰプロトコルのシーケンス番号を推測し、偽のセッションを確保し攻撃対象ホストのファイルに不正アクセスすること。

【０１０１】（２）ＳＭＴＰプロトコルのＤＥＢＵＧコマンドを使い、攻撃対象ホストのファイルに不正にアクセスすること。

【０１０２】（３）ＭＩＭＥを使って攻撃ホストのセキュリティ管理ファイルを書換え、攻撃ホストにパスワード無しでログインできるようにすること。

【０１０３】（４）電子メールやニュースを攻撃対象ホストの処理能力を超えて大量に送りつけ、ネットワーク機能を麻痺させること。

【０１０４】（５）telnetプロトコルで、root,guest等めぼしいアカウントにアクセスし、パスワードを適当に推測し、ログインを試みること。

【０１０５】（６）TFTPプロトコルを用いて、パスワード無しで攻撃対象ホストのファイルにアクセスすること。

【０１０６】以上のように構成された本実施形態のネットワーク不正解析システム５０によれば、次のような利点がある。

【０１０７】（１）アプリケーション層までのセッションの再構築を行うことができ、不正解析をおこなう者にとってわかり易いデータを取り扱えるようになった。すなわち、ネットワーク上でのパケットでのデータは細分化されているため解析を行うことが困難であるが、本実施形態のネットワーク不正解析システム５０ではアプリケーション層までのセッションの再構築を行っているので解析データを意味有るデータとすることができる。これにより、データ中の不正の有無を容易に判定することができる。しかも、ネットワークでの不正の多くはデータ部分に発生するので、このデータ部分の不正を検出することにより効率の良い不正解析を行うことができる。

【０１０８】（２）層毎の完全なモジュール化により、複数の種類のプロトコルを扱えるようになった。すなわち、ネットワークのプロトコルは図５に示す階層化モデル８００のようにモデル化でき、本実施形態のネットワーク不正解析システム５０はコンフィグレーションファイルの設定に基づきこのモデルを利用して不正の解析を実行するので、新たなプロトコルが開発されても、コンフィグレーションファイル及びデータ作成部５６の新たなプロトコルが対応する層を担当する一部のレイヤモジュールのみを変更することにより対応することができる。このため、データ作成部５６を新たに開発されたプロトコルに対応させるためにデータ作成部５６の全体を変更する必要はないので、プロトコル数の増大に容易に対応することができる。

【０１０９】（３）データ解析部での不正解析はコンフィグレーションファイルに記述した検知方法に基づいて行われるので、新たな種類の不正の発生をコンフィグレーションファイルの記述を変更するのみでデータ解析部のソフトウェア自体を変更することなく検出することができる。

【０１１０】（４）緩衝帯ネットワーク３との組み合わせにより、任意の通信を取り扱えるようになった。例えば、ＬＡＮ１のステーションや外部ネットワーク７が複数ある場合に、任意の送信元と受信先とについて不正解析を行うことができる。

【０１１１】（５）緩衝帯ネットワーク３としてホストから独立しているので、ホスト数の増加にも容易に対応できる。

【０１１２】以上のように本発明の第１の実施の形態によれば、ネットワークの不正解析が可能になる。

【０１１３】〔第２の実施の形態〕図１０に、本発明に係るネットワーク不正解析方法の第２の実施の形態を示す。この図１０において、ネットワーク不正解析システム５０は、中央演算処理装置が主記憶装置に記憶されたプログラムを処理することにより実現されるものであって、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワークにおける不正を解析するシステムである。なお、図１０中で、実線に矢印は「データの流れ」を、破線に矢印は「制御メッセージの流れ」をそれぞれ示している（図３０及び図３４～図３７でも同様）。

【０１１４】すなわち、ネットワーク不正解析システム５０は、データ収集／送信処理部Ｖ１１と、アナライザ管理部Ｖ１２と、プロトコル処理部Ｖ１３と、アプリケーションアナライザＶ２１と、プロトコルスタックＶ１０１と、ネットワークアプリケーションＶ２０１とから構成されている。ここで、データ収集／送信処理部Ｖ１１と、アナライザ管理部Ｖ１２と、プロトコル処理部Ｖ１３と、プロトコルスタックＶ１０１とは、ＯＳ空間Ｖ１において実装されている。また、アプリケーションアナライザＶ２１と、ネットワークアプリケーションＶ２０１とは、ユーザ空間Ｖ２に実装されている。

【０１１５】また、データ収集／送信処理部Ｖ１１は、例えば緩衝帯ネットワーク３で伝送されているパケットＰＴを取り込む収集処理を実行し、あるいはアナライザ管理部Ｖ１２からのパケットＰＴＡ２を整形してパケットＰＴＡ１を作成してネットワークに送信するデータ収集／送信工程を実行する。データ収集／送信処理部Ｖ１１及びデータ収集／送信工程は、それぞれ第１の実施形態でのデータ収集部５５及びデータ収集工程に相当する。

【０１１６】アナライザ管理部Ｖ１２は、データ収集／送信処理部Ｖ１１からのパケットＰＴについて各アプリケーションアナライザ毎にフィルタ処理やフォワード処理を行いパケットＰＴａを作成し、かつプロトコル処理部Ｖ１３からの送信データＤＴＡを整形してＰＴＡ２を

作成し、さらにプロトコル処理部Ｖ１３からの制御メッセージＣＭを受け取りアナライザ管理情報を更新するアナライザ管理工程を実行する。

【０１１７】プロトコル処理部Ｖ１３は、アナライザ管理部Ｖ１２からのパケットＰＴａをアプリケーションアナライザの指定するプロトコル処理モジュールで再構築処理をすることにより解析データＤＴを作成するプロトコル処理工程を実行し、また、アプリケーションアナライザＶ２１からの送信データＤＴＡ及び制御メッセージＣＭを受信して送出する処理を実行する。

【０１１８】これらアナライザ管理部Ｖ１３及びプロトコル処理部Ｖ１３は第１の実施形態でのデータ作成部５６に相当すると共に、アナライザ管理工程及びプロトコル処理工程は第１の実施形態でのデータ作成工程に相当する。

【０１１９】アプリケーションアナライザＶ２１は、プロトコル処理部Ｖ１３からの解析データＤＴに不正が発生しているか判定して解析結果ＣＤＣを出力しまた解析結果からデータＤＴＡ及び制御メッセージＣＭを作成するデータ解析工程を実行する。アプリケーションアナライザＶ２１及びデータ解析工程は、それぞれ第１の実施形態でのデータ解析部５７及びデータ解析工程に相当する。

【０１２０】プロトコルスタックＶ１０１は、データ収集／送信処理部Ｖ１１からのパケットＰＴｂを取り込んで処理することにより解析データＤＴｂを作成すると共に、ネットワークアプリケーションＶ２０１から送出データＤＴＢを受け取って処理して送出パケットＰＴＢを作成してデータ収集／送信処理部Ｖ１１に与えるデータ作成送出工程を実行する。

【０１２１】ネットワークアプリケーションＶ２０１は、プロトコルスタックＶ１０１からの解析データＤＴｂを取り込み所定の処理を実行して送出データを作成すると共に、送出データＤＴＢをプロトコルスタックＶ１０１に出力するネットワーク処理工程を実行する。

【０１２２】このようなネットワーク不正解析システム５０は、図１０に示すように、通常のネットワークアプリケーションによる通信について、データ収集／送信処理工程と、アナライザ管理工程と、プロトコル処理工程と、アナライザ工程とを実行すると共に、データ作成送出工程及びネットワーク処理工程を実行する。このようなネットワーク不正解析システム５０を構成する各要素により、第１の実施形態と同様の手法も用いて通信内容を解析した結果、不正行為が行われているセッションやホスト等を特定することができる。

【０１２３】図１１及び図１２に、上記ネットワーク不正解析システム５０の詳細構成を示す。この図１１において、実線に黒塗矢印は「データの流れ」を、破線に矢印は「制御メッセージの流れ」を、実線に細い矢印は「情報の参照／変更」をそれぞれ示している。

【０１２４】これらの図において、アナライザ管理部Ｖ１２は、データ送信処理部Ｖ１２ａと、メッセージ処理部Ｖ１２ｂと、フイルタ処理部Ｖ１２ｃと、フォワード処理部Ｖ１２ｄと、アナライザ管理情報Ｖ１２ｅとからなる。また、アナライザ管理情報Ｖ１２ｅには、アプリケーションアナライザＡ用の管理情報Ｖ１２ea、アプリケーションアナライザＢ用の管理情報Ｖ１２eb、及びアプリケーションアナライザＣ用の管理情報Ｖ１２ecを備えている。

【０１２５】上記データ送信処理部Ｖ１２ａは、例えばデータ収集／送信処理部Ｖ１１からのパケットＰＴを取り込み各アプリケーションアナライザ毎にフィルタ処理を行う。メッセージ処理部Ｖ１２ｂは、フィルタ処理部Ｖ１２ｃからのパケットＰＴを取り込み各アプリケーションアナライザ毎にフォワード処理を行う。アナライザ管理情報Ｖ１２ｅは、フィルタ処理部Ｖ１２ｃ及びフォワード処理部Ｖ１２ｄから参照されまたメッセージ処理部Ｖ１２ｂから参照及び更新される。メッセージ処理部Ｖ１２ｂは、プロトコル処理部Ｖ１３からのデータＤＴＡを取り込みまた制御メッセージＣＭを取り込みアナライザ管理情報Ｖ１２ｅを更新する。データ送信処理部Ｖ１２ａは、フォワード処理部からのパケットＰＴｆ及びメッセージ処理部からのパケットＰＴＡを取り込み整形を行いパケットＰＴＡ２を出力する。また、アナライザ管理情報Ｖ１２ｅは、例えばアプリケーションアナライザＡ（Ｖ２１ａ）用の管理情報Ｖ１２ｅａ及びアプリケーションアナライザＢ（Ｖ２１ｂ）用の管理情報Ｖ１２ｅｂ及びアプリケーションアナライザＣ（Ｖ２１ｃ）用の管理情報Ｖ１２ｅｃとから構成されている。

【０１２６】プロトコル処理部Ｖ１３は、プロトコル処理モジュールＶ１３ａと、プロトコル処理モジュールＶ１３ｃ１と、プロトコル処理モジュールＶ１３ｃ２とからなる。

【０１２７】プロトコル処理モジュールＶ１３ａは、例えば、アプリケーションアナライザ（Ａ）Ｖ２１ａによって指定される。プロトコル処理モジュールＶ１３ｃ１及びプロトコル処理モジュールＶ１３ｃ２は、アプリケーションアナライザ（Ｃ）Ｖ２１ｃによって指定される。なお、アプリケーションアナライザ（Ｂ）Ｖ２１ｂのように、指定するプロトコル処理モジュールが存在しない場合もある。

【０１２８】アプリケーションアナライザＶ２１は、例えば、アプリケーションアナライザ（Ａ）Ｖ２１ａと、アプリケーションアナライザ（Ｂ）Ｖ２１ｂと、アプリケーションアナライザ（Ｃ）Ｖ２１ｃとから構成されている。これらは、既に述べたが、ユーザ空間Ｖ２に存在する。

【０１２９】図１３に、アナライザ管理情報の例を示す。この図１３において、アナライザ情報格納用構造体ＳＴ１は、フィルタ処理部Ｖ１２ｃからプロトコル処理

部Ｖ１３に渡すパケットＰＴａの指定をするための情報や、フォワード処理部Ｖ１２ｄからデータ送信部Ｖ１２ａへ渡すパケットＰＴｆの指定をするための情報を書き込むことができるようになっており、例えば図１３に示すような内容のように記載される。

【０１３０】このように構成されたネットワーク不正解析システム５０の動作を図１４～図１７を参照して説明する。図１４及び図１５に、同システム５０におけるネットワーク４からのパケットを処理する場合の動作を説明するためのフローチャートを示す。図１６に、同システム５０におけるアプリケーションアナライザＶ２１からのデータを処理する場合の動作を説明するためのフローチャートを示す。図１７に、図１４～図１６に現れるデータ送信部Ｖ１２ａの動作を説明するためのフローチャートを示す。

【０１３１】図１４及び図１５に示すように、ネットワーク不正解析システム５０は、パケットを取り込む（Ｐ１）。取り込んだパケットについて、フィルタ処理部Ｖ１２ｃにおいて、未処理のアナライザが存在する場合は（Ｐ１１；Ｙｅｓ）、未処理のアナライザ情報を取得する（Ｐ１２）。未処理のアナライザが存在しない場合は（Ｐ１１；Ｎｏ）、フォワード処理部Ｖ１２ｄへパケットを送信する。未処理のアナライザ情報を取得したのち、その情報に従ってパケットがアナライザのフィルタリングルールを満たすか否かを判定し、満たす場合は（Ｐ１３；Ｙｅｓ）、パケットをプロトコル処理部へ送信する。満たさない場合は（Ｐ１３；Ｎｏ）、次のアナライザに対する処理に移る。

【０１３２】プロトコル処理部Ｖ１３は、フィルタ処理部Ｖ１２ｃからのパケットを受け取り、アナライザに対応するプロトコル処理モジュールがアナライザが解析しやすいデータ形式にパケットを処理し（Ｐ２１）、データをアナライザへ転送する（Ｐ２２）。

【０１３３】フォワード処理部Ｖ１２ｄは、フィルタ処理部Ｖ１２ｃから受け取ったパケットについて、未処理の禁止則が存在する場合（Ｐ３１；Ｙｅｓ）、未処理の禁止則を取得する（Ｐ３２）。未処理の禁止則が存在しない場合は（Ｐ３１；Ｎｏ）、パケットをデータ送信処理部Ｖ１２ａへ送る。未処理の禁止則を取得したのち、パケットが禁止則に合致するか否かを調べ、合致する場合（Ｐ３３；Ｙｅｓ）は、データを破棄し（Ｐ３４）、次のパケットを入力する。データが禁止則に合致しない場合（Ｐ３３；Ｎｏ）は、次の未処理の禁止則が存在するか調べる。そして、全ての禁止則に合致しない場合は、データをフォワードする。

【０１３４】図１６に示すように、メッセージ処理部Ｖ１２は、アナライザが送信したメッセージを受信する（Ｐ２）。受信したメッセージの内容を処理した後（Ｐ４１）、アナライザ管理情報に変更があった場合は（Ｐ４２；Ｙｅｓ）、アナライザ管理情報の変更処理を行う（Ｐ４３）。情報変更がなかった場合（Ｐ４２；Ｎｏ）、または、アナライザ管理情報の変更を完了した場合（Ｐ４２；Ｙｅｓ）、次にデータ送信が必要な場合（Ｐ４４；Ｙｅｓ）、データをデータ送信処理部Ｖ１２ａへ渡す。データ送信が不要な場合は（Ｐ４４；Ｎｏ）、何もしない。

【０１３５】図１７は、図１４～図１６に共通に現れるデータ送信処理部の動作を示したフローチャートである。図１７に示すように、データ送信処理部はデータを受け取り（Ｐ５１）、通信可能となるようにデータを整形し（Ｐ５２）、実際にネットワークへデータを送る（Ｐ５３）。

【０１３６】また、このフローチャートを使用すれば、複数の種類のアプリケーションアナライザを設定することにより、複数の種類のクラッキング等の不正アクセスを同時に監視できる。

【０１３７】図１８に、上述したネットワーク不正解析システム５０を適用した通信装置ＭＣＮＣを、ネットワークＮＴＷで接続された通信装置ＭＣＮＡ，ＭＣＮＢに適用した例を示す。

【０１３８】上述した実施の形態を備えた通信装置ＭＣＮＣは、ＯＳ空間にＣＡプロトコルスタックを実装し、ＣＡ通信ライブラリ及びアナライザをユーザ空間に実装したため、この発明をユーザーが簡単に利用できるユーザインタフェースを提供することができる。ここで、ＣＡプロトコルスタックとは、図１０に示すアナライザ管理部Ｖ１２及びプロトコル処理部Ｖ１３、または図３４に示すＵアナライザ管理部Ｖ３１及びＵプロトコル処理部Ｖ３２、あるいは図３６に示すプロトコルスタック＊Ｖ４１を意味する。

【０１３９】図２２に、UNIXのソケットライブラリの場合を例として、疑似コードにより、通信の解析を行う場合のプログラミングの実際を示す。

【０１４０】同図（ａ）に示すように、本発明の通信ライブラリでは、socket()関数の呼び出しにより、アプリケーションアナライザはCAプロトコルスタックと接続する。これは初期状態である。

【０１４１】そして、bind()関数の呼び出しにより、フィルタルールを登録してデータ収集状態に移行する。さらに、accept()関数は、フィルタルールに合うセッションが開始されるまでスリープする。目的のセッションが開始されると、accept()関数の呼び出しから戻り、新たな識別子new_fd を得る。このnew_fdを使ってセッションのデータを読み込むことができる。

【０１４２】ところが、new_fdを使い特定セッションの解析を行うと、新たなフィルタルールに合うセッションが現われたときに対応することができない。そこで、特定セッションの解析は別のプロセスで行うことになる。それがfork()コールである。fork()によりプロセスは親と子に別れる。子の場合、fork()の戻り値は０である。

親の場合は0ではない。子はnew_fdを使って特定セッションを解析して親は再びaccept()をコールしフィルタルールに合うセッションを待つ。

【０１４３】一方、図２２（ｂ）に示す従来の通信ライブラリでは、socket()関数の呼び出しにより、ネットワークアプリケーションはプロトコルスタックと接続する。そして、bind()関数の呼び出しによりサービスを指定する。さらに、accept()関数を呼び出して，クライアントからの接続を待つ。クライアントからの接続要求があるとaccept()関数の呼び出しから戻り、新たな識別子new_fdを得る。このnew_fdを使ってクライアントと通信することができる。

【０１４４】ところが、new_fd を使い特定クライアントと通信すると、新たなクライアントからの接続要求に答えることができない。そこで、特定クライアントとの通信は別のプロセスで行うことになる。そのため、fork()を使う。fork()によりプロセスは親と子に別れる。子の場合、fork()の戻り値は0である。親の場合は0ではない。子はnew_fdを使って特定クライアントと通信し、親は再びaccept()をコールしフィルタルールに合うセッションを待つ。

【０１４５】上述のように従来のネットワーク解析ツールでは独自のコードスタイルにならざるを得なかったが、本発明のプロトコルスタックと通信ライブラリによりネットワークアプリケーションと同様のスタイルのプログラミングでネットワーク解析ツールを作成することができるようになる。

【０１４６】図２３にUNIXのソケットライブラリの場合を例として、疑似コードにより、通信のハイジャックを行う場合のプログラミングの実際を示す。

【０１４７】同図に示すように、hijack()関数の呼び出しによりハイジャック状態に移行する。この状態ではnew_fdを使いデータを送信することができる(write()コール)。もちろん、データ収集状態の時に行えたデータ読み込みも継続して行える。write()コールの引き数に送信先というものがあるが、これでサーバまたはクライアントに対しての送信なのかを指定する。

【０１４８】従来はハイジャック機能の実現のために高度なプログラミング技術が必要で、また動作の安定するものは困難であった。本発明により、ネットワーク通信のハイジャックを行うツールをネットワークアプリケーションプログラムと同様のスタイルで、容易に開発することができるようになる。

【０１４９】さらに、上述したネットワーク不正解析システム５０のアプリケーションアナライザの出力例を図２４～図２６に示す。

【０１５０】図２４及び図２５に示す

```
ETHER:00:808:17:88:8d >> 00:a0:24:23:16:0d
IP:202.26.75.116 >> 202.26.75.71
TCP:40508 >> 23
```

の部分はホストA（IPアドレスは202.26.75.116）からホストB（IPアドレスは202.26.75.71）へ、telnet（サービスポート番号２３）で接続したことを意味する。ここでは、クライアントがホストAで、サーバがホストBである。また、SRC(source)で表わされるものがホストAで、DST（destination）で表わされるものがホストBである。

【０１５１】[src << (DST)]の部分は、DSTからSRCへデータが渡ってきたことを意味する。SRCからDSTへのデータは[(SRC) >> dst]と成る。そして、(id:4553)はこの通信の識別子である。<len:71>は、送られてきたデータの長さを表す。上記の場合は71バイトのデータを表す。

【０１５２】これらの図は、ネットワークのデータを読み込み表示するツールの一例である。ホストAがホストBにtelnetで接続し、ホストBが

```
BSDI BSD/OS 3.0 (netlog.nal.go.jp)(ttyp0)
login:
```

をホストAに送る。ホストAからrot という入力があり，ホストBはPassword:というデータをホストAに返す、そこで、ホストAからroot1という入力があり、ホストBはlogin incorrectを返している。

【０１５３】次に、図２６の表示内容について説明する。左のウインドウは解析対象を指定するウインドウである。EthernetアドレスやIPアドレス，TCPポート番号を入力できるフィールドがある。同図の例では、IPアドレス202.26.75.71の25番ポート宛の通信すべてを解析対象にしている。そして、左のウインドウの下半分に解析対象に合致したセッションが表示される。同図の例では、202.26.775.116から202.26.75.71あてのセッションが検出されている。検出されているセッション一覧のなかで、指定したものの詳細を別ウインドウに表示することができる。複数のセッションが存在する場合は、ウインドウをそれぞれに対応させて、複数開くことができる。

【０１５４】また、このウインドウが図の右側に表示されている。このウインドウの上部に通信に使用されているアドレスが表示され、中央部に通信の内容がリアルタイムで表示されている。最下部に２つのボタンがあり、[Kill Session]ボタンはセッションの強制終了を行い、[Hijack Session]はセッションのハイジャックを行う。この[Hijack Session]ボタンを押した後は、そのボタンの上のCmd to SrcやCmd to Dstフィールドにデータを入力し、それを通信の当事者に送ることができる。ハイジャック後も通信の当事者から出されたデータはウインドウの中央部分に表示される。

【０１５５】〔第３の実施の形態〕図２７に、同第３の実施の形態を示す。この図２３では、ネットワーク不正解析システム５０に複数のネットワークインターフェースを設けてマルチホーム化することができる。例えば２

つのネットワークインターフェースを設けてデュアルホーム化して別個のネットワーク４，５に接続されるときは、ＬＡＮ１と外部ネットワーク７との間の通信は必ずネットワーク不正解析システム５０の内部を通過することになる。このため、ネットワーク不正解析システム５０でのパケットの収集を取りこぼし無く行うことができる。これにより、ネットワークでの不正を高精度に検出することができる。

【０１５６】また、図２８に示すように、ネットワーク不正解析システム５０をマルチホーム化すると共に、データ解析部５７からデータ収集部５５へ解析結果をフィードバックさせるようにしても良い。なお、図２８では、データ作成部５６及びデータ解析部５７の具体的な図示は省略している。この場合、データ解析部５７の解析結果によってデータ収集部５５の処理が変化される。これにより、解析の結果、不正行為が行われているセッションやホスト等が特定できた場合、その通信についてはネットワーク不正解析システム５０内を通過させないようにデータ収集部５５を制御することができる。したがって、ネットワークでの不正のＬＡＮ１への侵入を防止することができる。

【０１５７】さらに、図２９に示すように、データ作成部５６を、層構造のレイヤフィルタ６$1_{1A}$，…，６$1_{kA}$，…，６$1_{nA}$を有するフィルタリング処理部５８と、層構造のレイヤ再構築部６$1_{1B}$，…，６$1_{kB}$，…，６$1_{nB}$を有する再構築処理部５９とを備えたものにすることができる。この場合、データ作成部５６では、フィルタリング処理部５８においてフィルタリング処理をレイヤの数だけ先にまとめて行い、その後、再構築処理部５９において各レイヤについての再構築処理を行う。このため、解析の対象にならないデータがより早く破棄されるため、不必要な再構築処理やメモリ占有が解消され、ネットワーク不正解析システム５０の動作の高速化を図ることができる。

【０１５８】また、上述した第１の実施形態及び第３の実施形態ではネットワーク不正解析システム５０は図示しないコンピュータシステムから構成されるものとしているが、これには限られない。例えば、上述したネットワーク不正解析方法のデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させるためのプログラムを記録したＣＤ－ＲＯＭやフロッピーディスク等のコンピュータ読み取り可能な記録媒体を使用して汎用コンピュータを作動させることによりネットワーク不正解析システムを実行することもできる。

【０１５９】ここでのプログラムは、具体的には、情報通信ステーションの間で階層化されたプロトコルにより通信を行うように構築されたネットワーク上で伝送されているパケットを取り込むデータ収集工程を実行するデータ収集手順と、階層化されたプロトコルに応じた階層化モジュールのパラメータを予め読み込んでおいたコンフィグレーションファイルで指定された情報に基づいて設定し、データ収集手順からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するデータ作成工程を実行するデータ作成手順と、予め読み込んでおいたコンフィグレーションファイルで指定された内容を基にデータ作成手順からの解析データに不正が発生しているか判定するデータ解析工程を実行するデータ解析手順とをコンピュータに実行させるためのものである。

【０１６０】また、上述した実施形態ではデータ収集工程とデータ作成工程とデータ解析工程とを汎用コンピュータに実行させているが、これには限られずこれらの工程を専用のコンピュータから成る独立した装置に実行させるようにしても良い。さらに、上述した実施形態では、これらデータ収集工程とデータ作成工程とデータ解析工程とをコンピュータに実行させているが、これには限られずこれらの工程をシーケンス回路に実行させるようにしても良い。いずれの場合も、データ作成工程においてデータ収集工程からのパケットを各階層化モジュールでフィルタリングしてパケットの細分化されたデータを元の単位に再構築することにより解析データを作成するので、データ解析工程ではデータとして意味のある再構築後の解析データを解析対象とすることができる。このため、データ部分に発生した不正を容易に判別することができる。

【０１６１】〔第４の実施の形態〕図３０に、同第４の実施の形態を示す。この図３０に示す通信システムは、ネットワーク４、５の間に図１０に示すネットワーク不正解析システム５０を適用したものである。すなわち、ネットワーク不正解析システム５０は、データ収集／送信処理部Ｖ１１に、ネットワーク４と他のネットワーク５とを接続し、ネットワーク４とデータ収集／送信処理部Ｖ１１との間で通信をし、ネットワーク５とデータ収集／送信処理部Ｖ１１との間で通信をするようにデュアルホーム化したものである。

【０１６２】この図３０に示すシステムでは、通信装置ＭＣＮＡと通信装置ＭＣＮＢとの間の通信は必ずネットワーク不正解析システム５０を備えた通信装置ＭＣＮＣを通過することになる。例えば、図３１に示すように、通信装置ＭＣＮＡから通信内容[Hello B!]、通信相手方[A->B]なるパケットが送出されてくると、通信装置ＭＣＮＣは、そのパケットをＣＡプロトコルスタックに取り込み、ＣＡ通信ライブラリを介してアナライザに通信内容[Hello B!]を伝える。ここで、不正がない場合には、同一内容[Hello B!]に通信相手方[A->B]なるパケットを通信装置ＭＣＮＢに伝送する。

【０１６３】次に、通信に不正があると判断したときには、通信装置ＭＣＮＣはハイジャック状態になる。このとき、図３２に示すように、通信装置ＭＣＮＡから通信

内容[Hi B!]、通信相手方[A->B]なるパケットが送られてきて、また、通信装置ＭＣＮＢから通信内容[Hello A!]、通信相手方[B->A]なるパケットが送られてきたとすると、これらはアナライザに取り込まれる。

【０１６４】図３３に示すように、アナライザは今までの通信内容に基づいて、通信装置ＭＣＮＡに送信すべき通信内容[Oh A!]と通信装置ＭＣＮＢに送信すべき通信内容[Bye B!]を作成する。そして、これら内容をアナライザからＣＡプロトコルスタックに渡す。プロトコルスタックは、通信内容[Oh A!]は通信相手方[B->A]を付加して送出し、通信内容を[Bye B!]は通信相手方[A->B]を付加して送出する。

【０１６５】このようにしているので、通信内容を確実に収集でき、かつ、ハイジャックも確実に実行することができる。

【０１６６】ここで、図１９及び図２０に、この実施の形態が実現するハイジャック機能をネットワーク制御装置に適用した例を示す。図２１に、ネットワーク制御装置の動作例を示す。

【０１６７】この図１９（ａ）において、通信当事者ＴＣＮＡ，ＴＣＮＢとの間にネットワーク制御装置ＮＷＣＴが介在している通信システムにおいて、ネットワーク制御装置ＮＴＣＴにアプリケーションアナライザＶ２１から制御メッセージＣＭとしてフィルタルータ登録がなされる。このとき、ネットワーク制御装置ＮＷＣＴに保持されるアプリケーションアナライザの状態は、図２１に示すように、初期状態ＳＴＳαからデータ収集状態ＳＴＳβに移行する。

【０１６８】すると、アナライザ管理部Ｖ１２は、図１９（ｂ）に示すように、ネットワーク制御装置ＮＴＣＴを介して通信当事者ＴＣＮＡ，ＴＣＮＢのデータを収集することになる。ネットワーク制御装置ＮＷＣＴは、図２１に示すように、データ収集状態ＳＴＳβにある。

【０１６９】ここで、アナライザ管理部Ｖ１２が通信に不正を検出したときに、その程度が小さいものについては、図２０（ａ）に示すようにネットワーク制御装置ＮＷＣＴを中断制御して転送中断にする。このとき、ネットワーク制御装置ＮＴＣＴは、図２１に示すように、データ収集状態ＳＴＳβから転送中断状態ＳＴＳγに移行する。

【０１７０】ネットワーク制御装置ＮＴＣＴは、転送中断状態ＳＴＳγにおいて、収集したデータを上述した方法で解析し、不正がなければ、転送中断状態ＳＴＳγからデータ収集状態ＳＴＳβに移行する。これにより、システムは、再び、図１９（ｂ）の状態に移行する。

【０１７１】一方、　ネットワーク制御装置ＮＴＣＴは、転送中断状態ＳＴＳγにおいて、収集したデータを上述した方法で解析し、不正があると判断したときには、図２１に示すように、ハイジャック状態ＳＴＳδに移行させる。この結果、図２０（ｂ）に示すように、通信当事者ＴＣＮＡはネットワーク制御装置ＮＴＣＴを介してアプリケーションアナライザＶ２１と通信し、また、通信当事者ＴＣＮＢはアナライザ管理部Ｖ１２と通信することになる。しかしながら、通信当事者ＴＣＮＡ及び通信当事者ＴＣＮＢ同士は互いの通信を行っているものと錯覚することになる。

【０１７２】なお、アナライザ管理部Ｖ１２がデータ収集状態ＳＴＳβにあるときに、明らかに不正がある通信であると判断したものについては、図２１に示すように、データ収集状態ＳＴＳβからハイジャック状態ＳＴＳδに直ちに移行させる。これにより、通信当事者ＴＣＮＡ、ＴＣＮＢは、図１９（ｂ）の状態から図２０（ｂ）の状態に移行することになる。

【０１７３】このように、通信当事者ＴＣＮＡ、ＴＣＮＢの通信をアナライザ管理部Ｖ１２で監視して、通信に不正を発見したときには、直ちにハイジャック状態にすることにより、不正な通信が行われることを防止することができる。

【０１７４】換言すると、このようなネットワーク不正解析システム５０を構成する各要素により、通信内容を解析した結果、不正行為が行われているセッションやホスト等を特定することができた場合には、その通信については当該システム５０内を通過させないようしたりまた通信のハイジャックを行うようにアナライザ管理部Ｖ１２を制御することができる。したがって、ネットワークでの不正のＬＡＮ１への侵入を防止することができる。

【０１７５】なお、上述の実施形態は本発明の好適な実施の一例ではあるがこれに限定されるものではなく本発明の要旨を逸脱しない範囲において種々変形実施可能である。

【０１７６】例えば、ネットワーク３に接続されたネットワーク不正解析システム５０については、図３４に示すように、Ｕアナライザ管理部Ｖ３１とＵプロトコル処理部Ｖ３２をユーザ空間Ｖ２で実装するようにしてもよい。この場合、データ収集／送信処理部Ｖ１１、プロトコルスタックＶ１０１については、図１０の構成と同様にＯＳ空間Ｖ１に実装しておくものとする。

【０１７７】また、ネットワーク４，５に接続されたデュアルホーム化したネットワーク不正解析システム５０については、図３５に示すように、Ｕアナライザ管理部Ｖ３１とＵプロトコル処理部Ｖ３２をユーザ空間Ｖ２で実装するようにしてもよい。この場合、データ収集／送信処理部Ｖ１１、プロトコルスタックＶ１０１については、図３０の構成と同様にＯＳ空間Ｖ１に実装しておくものとする。

【０１７８】あるいは、図３４及び図３５の実施形態で、データ収集／送信処理部Ｖ１１やプロトコルスタックＶ１０１についてもユーザ空間Ｖ２で実装するようにしてもよい。

【０１７９】また、ネットワーク３に接続されたネットワーク不正解析システム５０について、図３６に示すように、既存のプロトコルスタックを改良してプロトコルスタック＊Ｖ４１にし、このプロトコルスタック＊Ｖ４１をＯＳ空間Ｖ１に実装することにより、同様の作用効果を実現することができる。

【０１８０】さらにまた、ネットワーク４，５に接続されたネットワーク不正解析システム５０について、図３７に示すように、既存のプロトコルスタックを改良してプロトコルスタック＊Ｖ４１にし、このプロトコルスタック＊Ｖ４１をＯＳ空間Ｖ１に実装することにより、同様の作用効果を実現することができる。

【０１８１】なお、アナライザ管理部やプロトコル管理部のみならずアプリケーションアナライザをもＯＳ空間Ｖ１に実装することにより、同様の作用効果を実現することができる。

【０１８２】また、上述した第２の実施形態及び第４の実施形態ではネットワーク不正解析システム５０は図示しないコンピュータシステムから構成されるものとしているが、これには限られない。例えば、上述したネットワーク不正解析方法のデータ収集／送信処理工程と、アナライザ管理工程と、プロトコル処理工程と、アナライザ工程とをコンピュータに実行させるためのプログラムを記録したＣＤ－ＲＯＭやフロッピーディスク等のコンピュータ読み取り可能な記録媒体を使用して汎用コンピュータを作動させることによりネットワーク不正解析システムを実行することもできる。

【０１８３】ここでのプログラムは、具体的には、ネットワークに対してパケットを送受信できるデータ収集／送信処理手順と、制御メッセージによって書き換えられるアナライザ管理情報を基にデータ収集／送信処理工程との間でパケット通信を行うとともに、通信に不正が検知されたときにはパケットでもって通信当事者と個々に通信して通信当事者間の通信をハイジャックするハイジャック機能を備えたアナライザ管理手順と、アナライザ管理手順から得たパケットから解析データを再構築するとともに、制御メッセージ及びデータをアナライザ管理手順に伝送するプロトコル処理手順と、プロトコル処理手順から取り込んだ解析データに不正がないか判断するとともに、その判断結果に応じて制御メッセージ及びデータを作成してプロトコル処理手順に送出するアナライザ手順とをコンピュータに実行させるためのものである。

【０１８４】同様に、上述の各工程に加えてデータ作成送出工程とネットワーク処理工程をもコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体を使用して汎用コンピュータを作動させることによりネットワーク不正解析システムを実行することもできる。ここでのプログラムは、具体的には、上述の各手順に加えてデータ収集／送信処理手順からのパケットを取込み所定の処理をして解析データとし、送出データを受け取って送出パケットにしてデータ収集／送信処理手順に与えるデータ作成送出手順と、データ作成送出手順から解析データを受け取り所定の処理を実行するとともに、所定の処理をされた送出データをデータ作成送出手順に与えるネットワーク処理手順とをコンピュータに実行させるためのものである。

【０１８５】また、上述した各実施形態ではデータ収集／送信処理工程と、アナライザ管理工程と、プロトコル処理工程と、アナライザ工程との各工程、あるいはこれらに加えてデータ作成送出工程とネットワーク処理工程を汎用コンピュータに実行させているが、これには限られずこれらの工程を専用のコンピュータから成る独立した装置に実行させるようにしても良い。さらに、上述した実施形態では、これらの工程をコンピュータに実行させているが、これには限られずシーケンス回路に実行させるようにしても良い。いずれの場合も、ネットワークに発生した不正を容易に判別してハイジャック機能を実行することができる。

【０１８６】

【発明の効果】以上説明したように請求項１記載のネットワーク通信の監視・制御方法及び請求項４記載のネットワーク通信の監視・制御装置によれば、パケットから解析データを再構築して解析できるので、再構築後のデータにより不正の判断を行うことができる。また、デュアルホームホストの採用によりハイジャック機能を実現できるので、ネットワークでの不正を防止することができる。

【０１８７】また、請求項３記載のネットワーク通信の監視・制御方法及び請求項６記載のネットワーク通信の監視・制御装置によれば、ユーザ空間にアプリケーションとして実装する場合に比べて優先的に実行されると共にメモリ等の使用頻度が非常に少なくなるので、処理速度を格段に向上させることができる。

【０１８８】したがって、本発明のネットワーク通信の監視・制御方法によれば以下の効果を得ることができる。

（１）オペレーティングシステムのプロトコルスタックの拡張部分が用意する手段を用いることにより、任意の情報通信ステーション間の通信を解析でき、簡便なデータ解析が可能となる。すなわち、データの解析者自らが、ネットワーク上の細分化されたデータをセッション単位にまで再構築する必要がなく、オペレーティングシステムの機能を呼び出すのみで任意の通信を任意のデータ形式で参照することが可能となる。

【０１８９】また、オペレーティングシステムの機能としてデータ参照機能が実現されているため、汎用的なインターフェースとなっており、簡便さや拡張性に富んだ実現方法となっている。

【０１９０】（２）上記（１）の機能で発見された不正

通信のセッションについて、オペレーティングシステムの用意する手段により、通信のハイジャックが可能となっており、不正通信を簡便に防止できる。これは、オペレーティングシステムの機能を呼び出すのみで対象としている通信を二つの独立した通信分割し、それぞれの通信に対して、不正通信の詳細な解析を行うための通信を生成することが可能となる。

【０１９１】また、上述したように本発明に係るネットワーク通信の監視・制御装置によれば、次のような利点がある。

（１）オペレーティングシステムのプロトコルスタックの拡張部分が用意する手段を用いることにより、任意の情報通信ステーション間の通信を解析でき、簡便なデータ解析が可能となる。すなわち、データの解析者自らが、ネットワーク上の細分化されたデータをセッション単位にまで再構築する必要がなく、オペレーティングシステムの機能を呼び出すのみで任意の通信を任意のデータ形式で参照することが可能となる装置を提供できる。

【０１９２】（２）不正通信に対しては、オペレーティングシステムの用意する手段により、通信のハイジャックが可能となっており、不正通信を簡便に防止できる装置を提供できる。

【０１９３】さらに、上記本発明に係るネットワーク通信の監視・制御プログラムを記録したコンピュータ読み取り可能な記録媒体によれば、コンピュータに読み込ませることにより、オペレーティングシステムのプロトコルスタックの拡張部分が用意する手段を用いることが可能となり、任意の情報通信ステーション間の通信を解析でき、簡便なデータ解析が可能となる。

【図面の簡単な説明】

【図１】本発明のネットワーク不正解析方法が適用されたネットワーク不正解析システムの実施の形態を示すブロック図である。

【図２】ネットワーク不正解析システムとネットワークとの接続を示すブロック図である。

【図３】ネットワーク不正解析システムの実施の形態の概略を示すブロック図である。

【図４】同実施の形態で使用するコンフィグレーションファイルの例を示す説明図である。

【図５】同実施の形態にプロトコルの階層化の例を説明するための図である。

【図６】同実施の形態の動作を説明するためのフローチャートである。

【図７】同実施の形態の動作を説明するための図である。

【図８】同実施の形態の動作を説明するための図である。

【図９】同実施の形態で処理した結果を示す図である。

【図１０】同実施の形態におけるネットワーク不正解析システムの実施の形態の概略を示すブロック図である。

【図１１】同実施の形態におけるネットワーク不正解析システムの実施の形態の詳細を示すブロック図である。

【図１２】同実施の形態におけるネットワーク不正解析システムの実施の形態の詳細を示すブロック図である。

【図１３】同実施の形態で使用する構造体の例を示す説明図である。

【図１４】同実施の形態の動作を説明するためのフローチャートである。

【図１５】同実施の形態の動作を説明するためのフローチャートである。

【図１６】同実施の形態の動作を説明するためのフローチャートである。

【図１７】同実施の形態の動作を説明するためのフローチャートである。

【図１８】同実施の形態の動作を説明するための図である。

【図１９】同実施の形態における通信ハイジャック機能の動作を説明するための図であり、（Ａ）は初期状態、（Ｂ）はデータ収集状態を示す。

【図２０】同実施の形態における通信ハイジャック機能の動作を説明するための図であり、（Ａ）は転送中断状態、（Ｂ）はハイジャック状態を示す。

【図２１】同実施の形態におけるネットワーク制御装置の動作状態遷移を説明するための図である。

【図２２】同実施の形態の通信監視用のプログラミングスタイルの疑似コードを示す説明図であり、（Ａ）は本発明の通信ライブラリについて、（Ｂ）は従来の通信ライブラリについて示す。

【図２３】同実施の形態の通信ハイジャック用のプログラミングスタイルの疑似コードを示す説明図である。

【図２４】同実施の形態で処理した結果を示す説明図である。

【図２５】同実施の形態で処理した結果を示す説明図である。

【図２６】同実施の形態で処理した他の結果を示す説明図である。

【図２７】ネットワーク不正解析システムの他の実施形態を示すブロック図である。

【図２８】ネットワーク不正解析システムの別の実施形態を示すブロック図である。

【図２９】ネットワーク不正解析システムのさらに他の実施形態を示すブロック図である。

【図３０】同実施の形態におけるネットワーク不正解析システムの実施の形態の概略を示すブロック図である。

【図３１】同実施の形態における通信動作の例を示す説明図である。

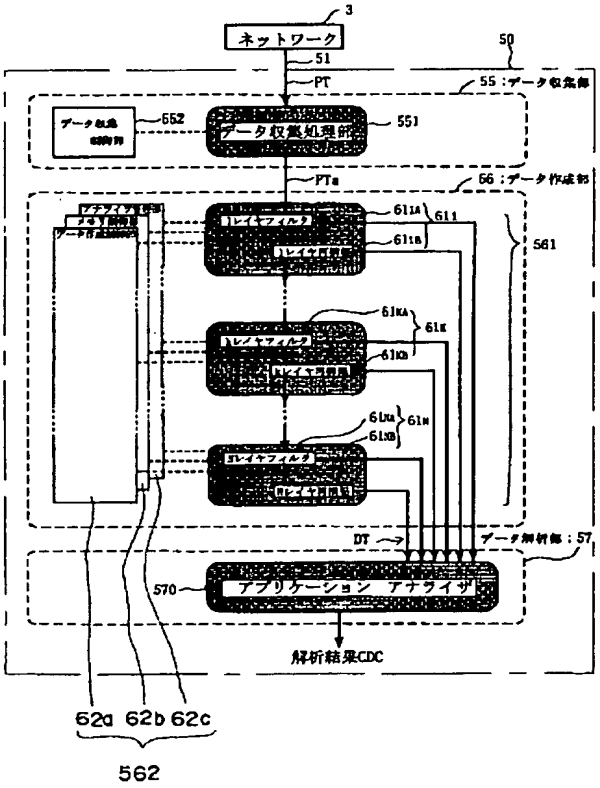
【図３２】同実施の形態における通信動作のうち通信ハイジャックの一態様例を示す説明図である。

【図３３】同実施の形態における通信動作のうち通信ハイジャックの他の態様例をを示す説明図である。

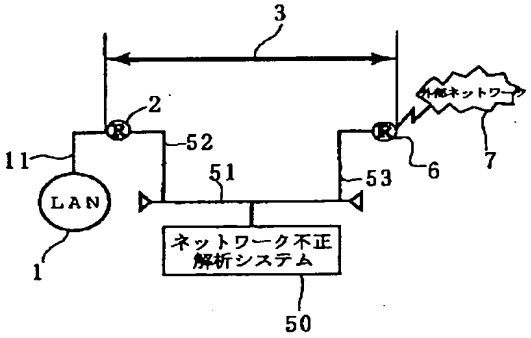
【図３４】同他の実施の形態におけるオペレーティングシステム空間の実装例を示すブロック図である。
【図３５】同他の実施の形態におけるオペレーティングシステム空間の他の実装例を示すブロック図である。
【図３６】同他の実施の形態におけるオペレーティングシステム空間のさらに他の実装例を示すブロック図である。
【図３７】同他の実施の形態におけるオプレーティングシステム空間のさらに他の実装例を示すブロック図である。
【図３８】従来のパケット単位の監視ツールの構成例を示すブロック図である。
【図３９】従来の代理サーバ形式の監視ツールの構成例を示すブロック図である。
【符号の説明】

１　ＬＡＮ
３　緩衝帯ネットワーク
７　外部ネットワーク
５０　ネットワーク不正解析システム
５５　データ収集部
５６　データ作成部
５７　データ解析部
Ｖ１　オペレーティングシステム空間
Ｖ２　ユーザ空間
Ｖ１１　データ収集／送信処理部
Ｖ１２　アナライザ管理部
Ｖ１３　プロトコル処理部
Ｖ２１　アプリケーションアナライザ
Ｖ１０１　プロトコルスタック
Ｖ２０１　ネットワークアプリケーション

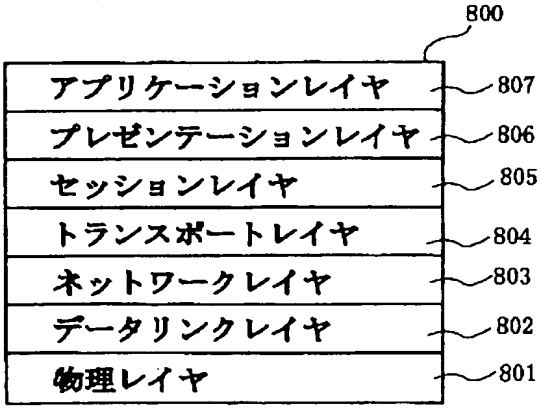
【図１】



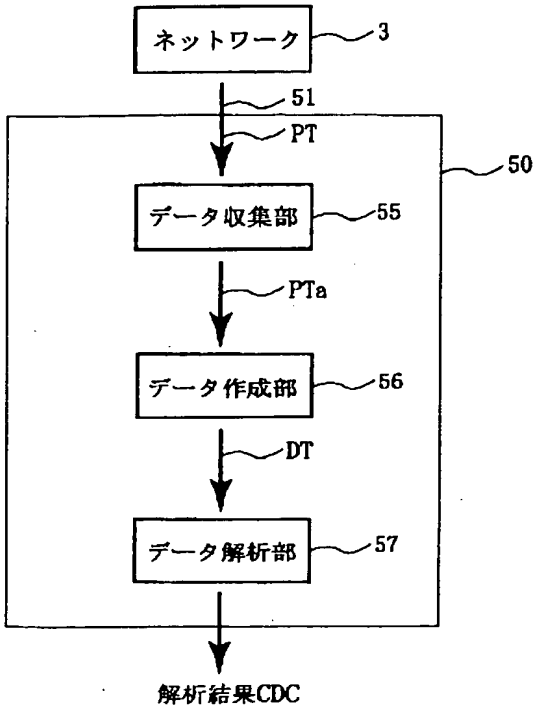
【図２】



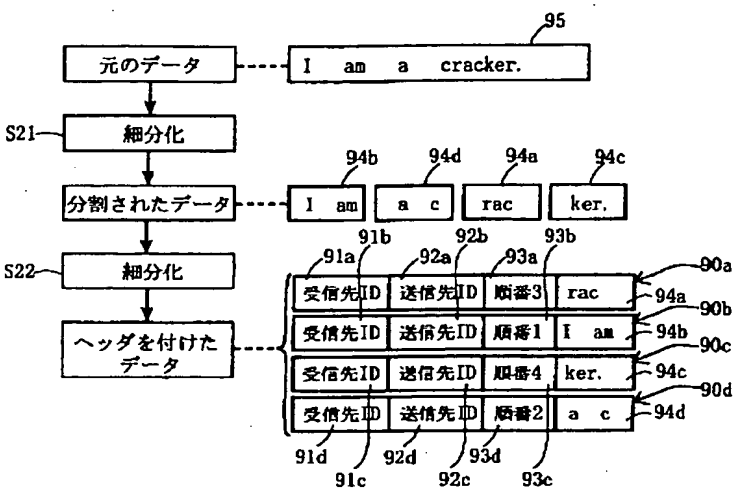
【図５】



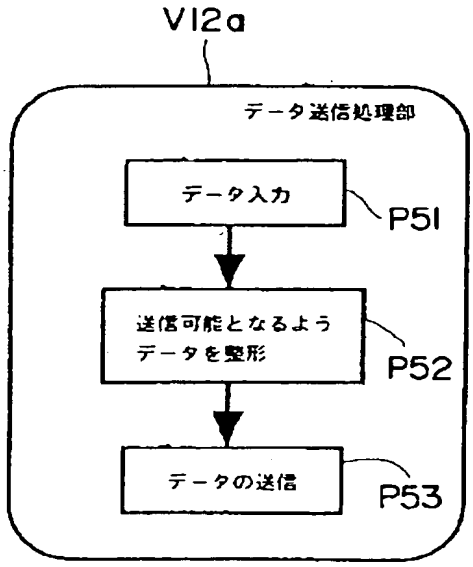
【図３】



【図７】



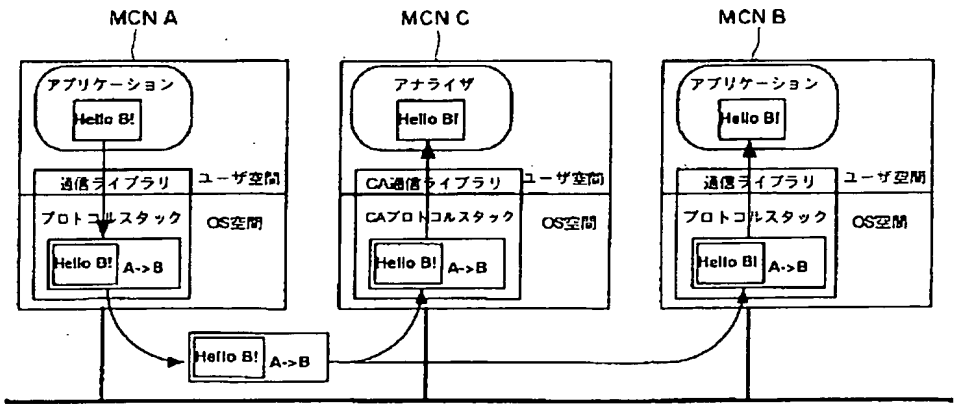
【図１７】



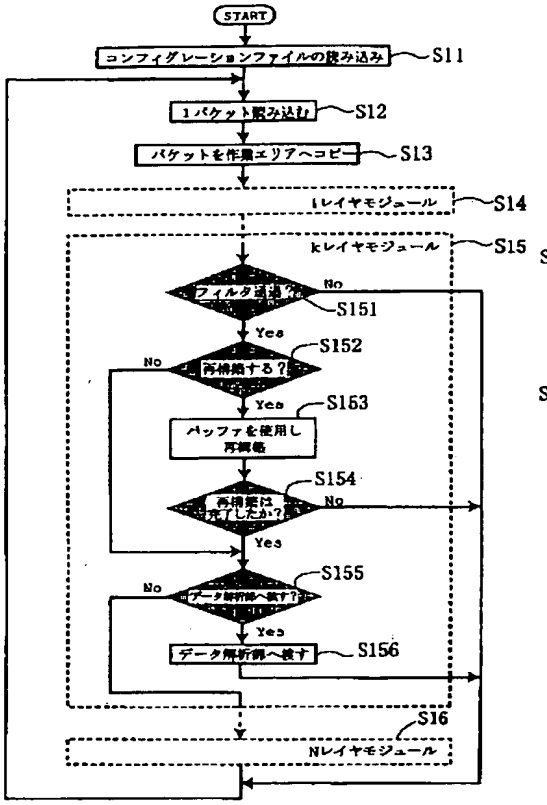
【図４】

```
500
#-------------------------------------------------------------------#
# Filter for login Analyzer                                         #
#-------------------------------------------------------------------#
filterset {
    physical  = { ether: * <-> aa:bb:cc:xx:yy:zz }
    network   = { ip: * <-> 202.26.95.68 }
    transport = { tcp: * <-> 23 }
    analyzer  = { login-A login.conf -log login.log -dump login.dump}
}
```

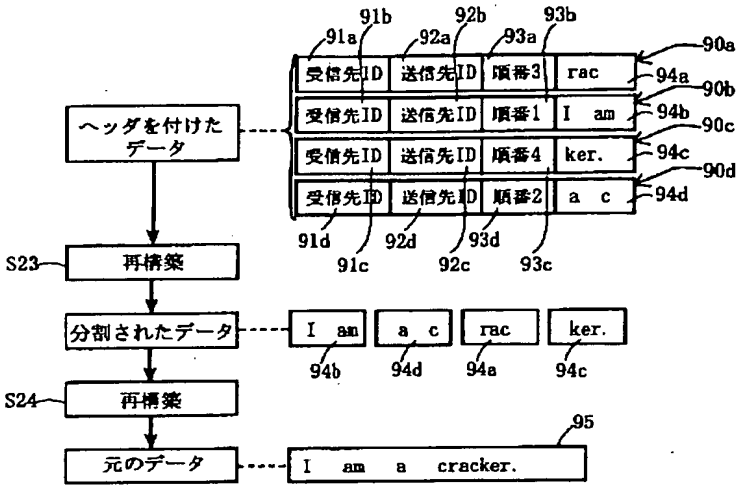
【図１８】



【図６】



【図８】



【図２２】

（ａ）本発明の通信ライブラリ

```
int fd,new_fd;
fd=socket();
bind(fd,監視対象のアドレスルール);
while(1){
   new_fd=accept(fd);
   if(fork() == 0){
      close(fd);
      new_fdを使ってサーバ～クライアントのデータ通信を解析する
   }
   close(new_fd);
}
```

（ｂ）従来の通信ライブラリ（サーバの場合）

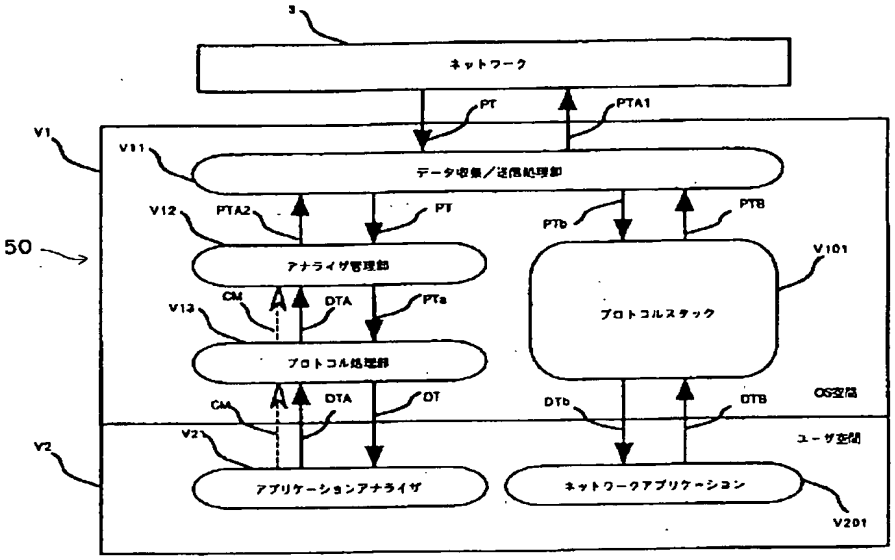
```
int fd,new_fd;
fd=socket();
bind(fd,開設するポート);
while(1){
   new_fd=accept(fd);
   if(fork() == 0){
      close(fd);
      new_fdを使ってクライアントとデータ通信を行う
   }
   close(new_fd);
}
```

【図９】

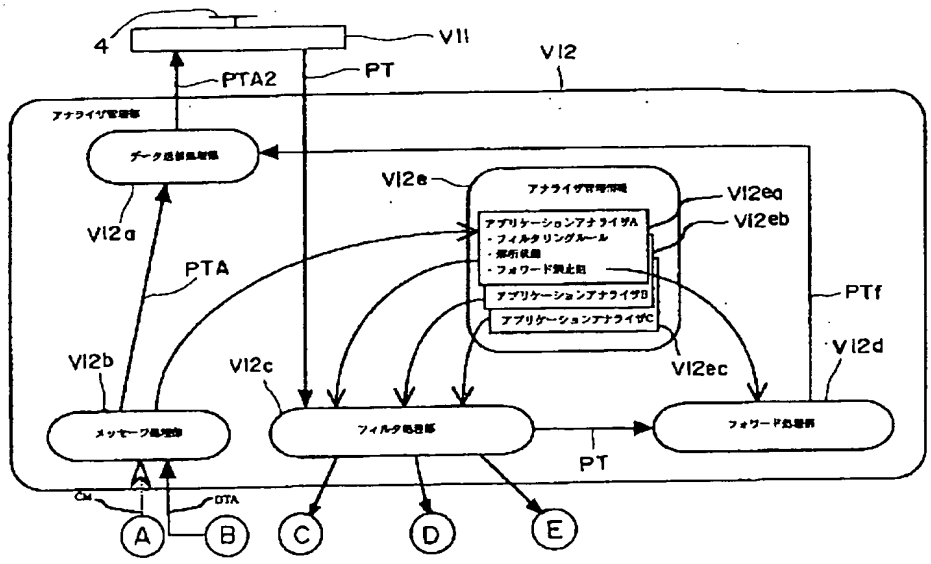
900

```
-------- Cracking Data contents -------------------------
Date                 : Dec 26 13:28:00 1996
Server Address       : 202.26.95.68:23
Client Address       : 202.26.95.69:1024
Defhost Name         : host1
Login Times          : Threshold User = 0  Threshold System = 3
Easy Password Used   : NO

-------- Command Details --------------------------------
S :
S : Welcome to mail.nal.go.jp (ttyp4)
S :
S : login:
C : root
S : Password:
C : rootS
S : Login incorrect
S : login:
C : root
S : Password:
C : root
```

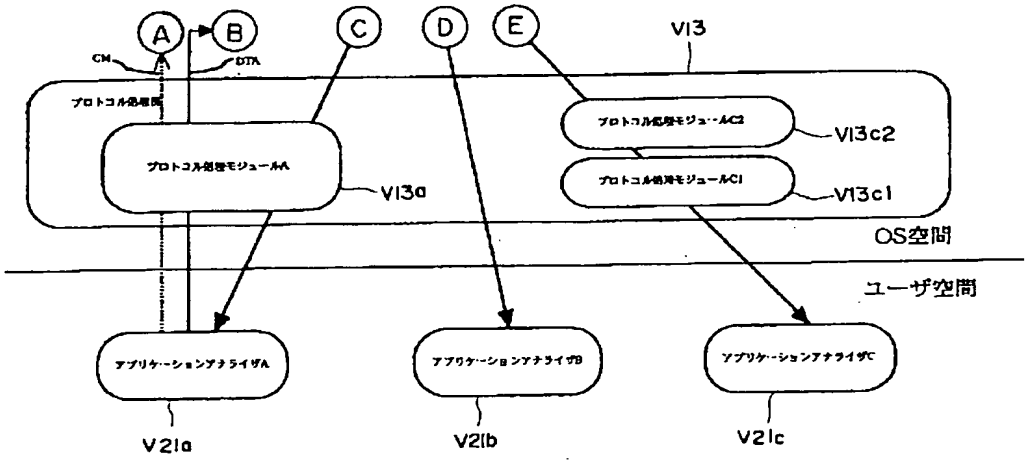
【図１０】


3
ネットワーク
PT
PTA1
V1
V11
データ収集／送信処理部
V12
PTA2
PT
PTb
PTB
50
アナライザ管理部
V101
プロトコルスタック
CM
A
DTA
PTa
V13
プロトコル処理部
CM
A
DTA
DT
DTb
DTB
OS空間
ユーザ空間
V2
V21
アプリケーションアナライザ
ネットワークアプリケーション
V201

【図１１】


4
V11
V12
PTA2
PT
アナライザ管理部
データ送受信処理部
V12a
V12e
アナライザ管理情報
V12ea
V12eb
アプリケーションアナライザA
・フィルタリングルール
・解析結果
・フォワード禁止処
アプリケーションアナライザB
アプリケーションアナライザC
PTA
PTf
V12d
V12b
V12c
V12ec
メッセージ処理部
フィルタ処理部
フォワード処理部
PT
CM
DTA
A
B
C
D
E

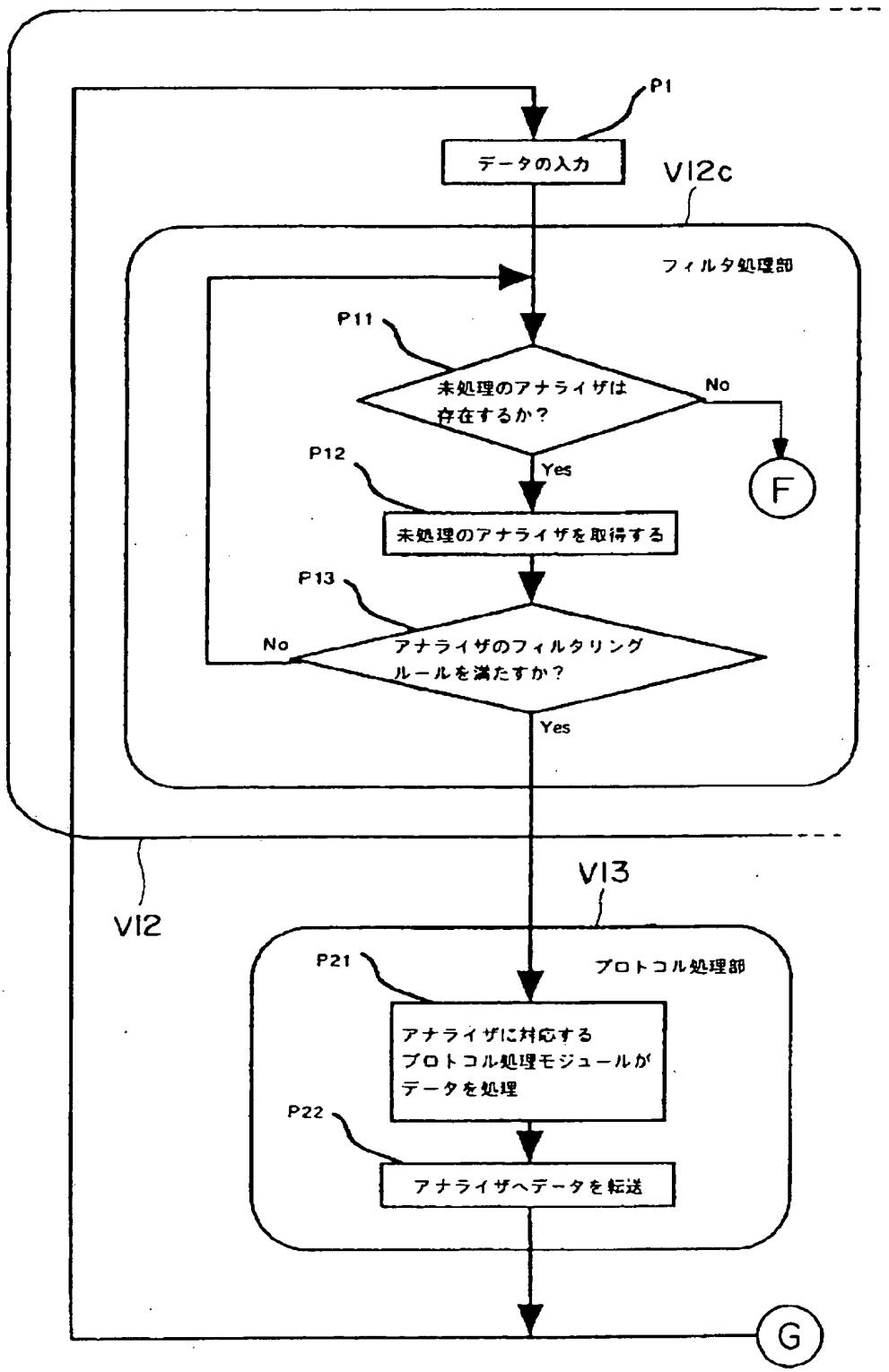
【図１２】



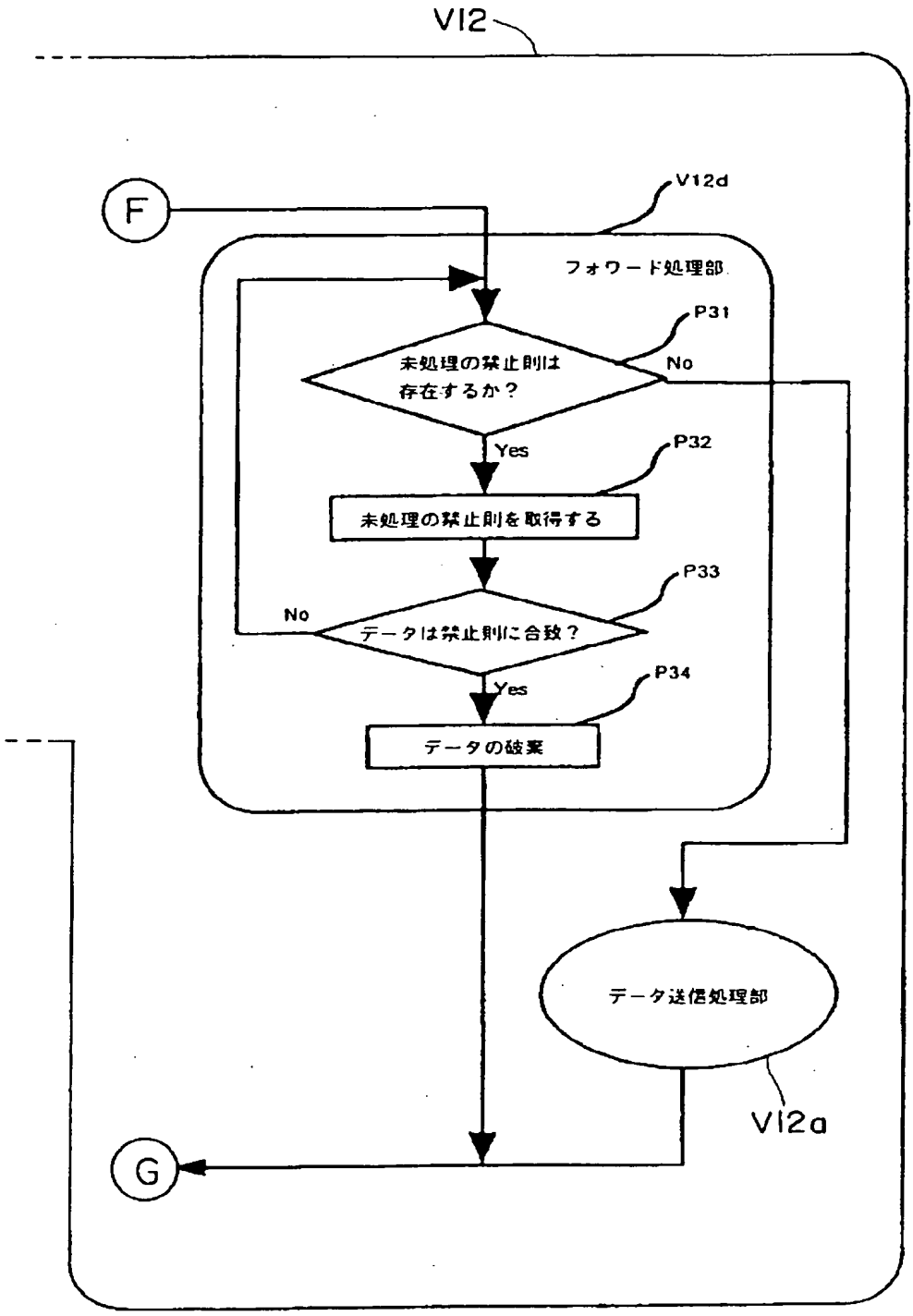
【図１３】

```
struct ca_filter {
        char    dir;            /* direction */

        /*------------------------------------------------------------------*/
        /* datalink layer                                                   */
        /*------------------------------------------------------------------*/
        char    dlk_id;
        union {
                struct ether_filter     ether;
        } dlk_f;

        /*------------------------------------------------------------------*/
        /* network layer                                                    */
        /*------------------------------------------------------------------*/
        char    net_id;
        union {
                struct ip_filter        ip;
                struct arp_filter       arp;
        } net_f;

        /*------------------------------------------------------------------*/
        /* transport layer                                                  */
        /*------------------------------------------------------------------*/
        char    tra_id;
        union {
                struct tcp_filter       tcp;
                struct udp_filter       udp;
        } tra_f;
};

struct ca_endpoint {
        queue_t*                qptr;           /* points to AA */
        short                   stat;           /* status */
        struct ca_filter        filter;         /* filtering rule */
        struct ca_filter        nf_filter;      /* no-forward filtering rule */
        int                     id;             /* identifier */
        int                     fd;             /* file descriptor */
        int                     bufcid;
        struct ca_endpoint*     ca_e;           /* used in accept */
        struct ca_eopt          opt;            /* option */
};
```

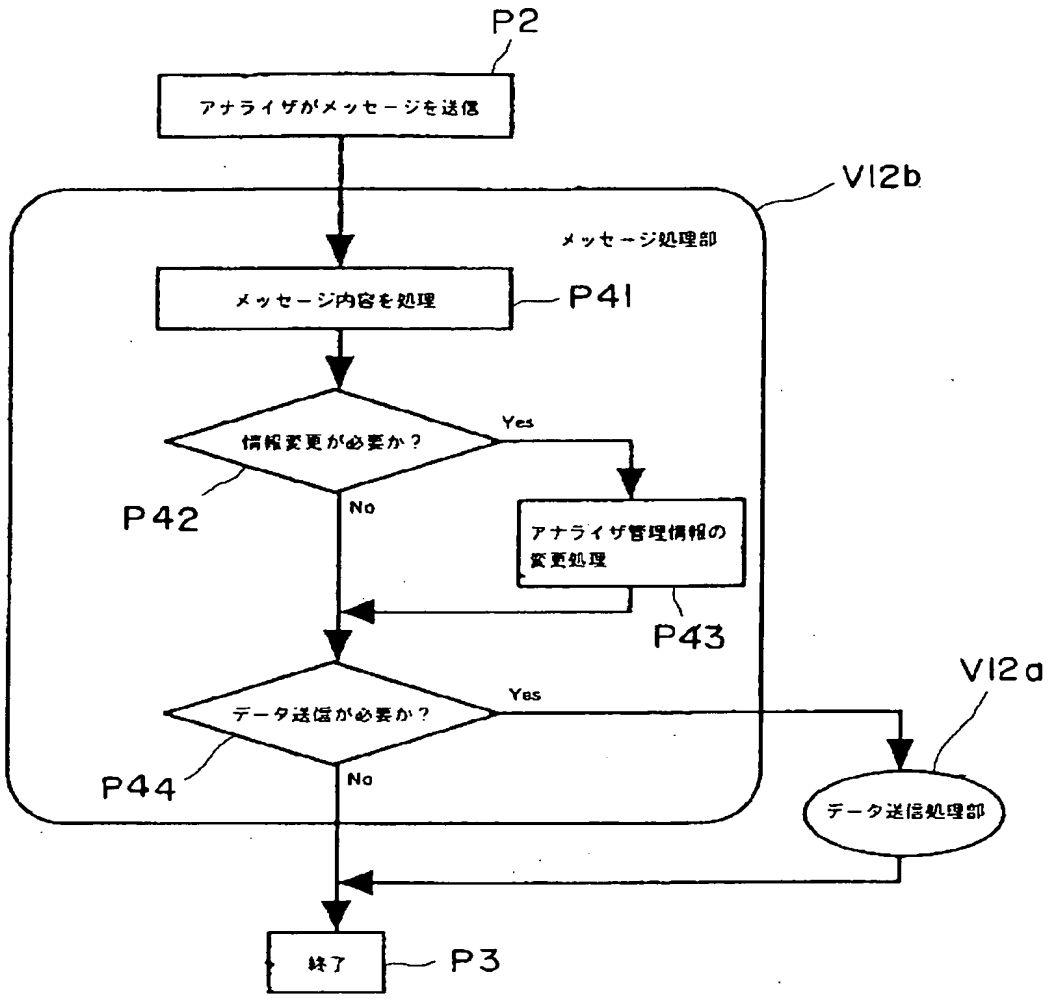
【図１４】


P1
データの入力
V12c
フィルタ処理部
P11
未処理のアナライザは
存在するか？
No
Yes
F
P12
未処理のアナライザを取得する
P13
No
アナライザのフィルタリング
ルールを満たすか？
Yes
V12
V13
P21
プロトコル処理部
アナライザに対応する
プロトコル処理モジュールが
データを処理
P22
アナライザへデータを転送
G

【図１５】


V12
V12d
F
フォワード処理部
P31
未処理の禁止則は
存在するか？
No
Yes
P32
未処理の禁止則を取得する
P33
No
データは禁止則に合致？
Yes
P34
データの破棄
データ送信処理部
V12a
G

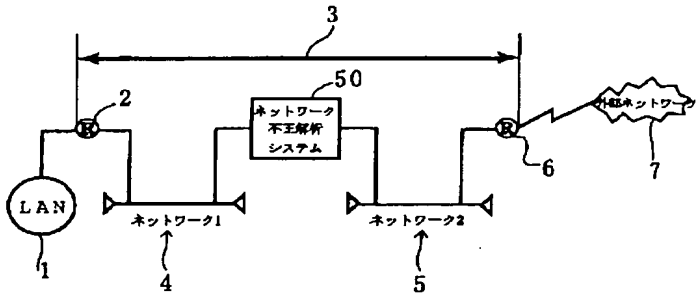
【図１６】



【図２３】

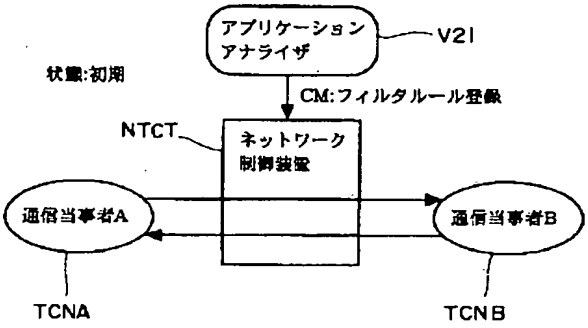
```
int fd,new_fd;
fd=socket();
bind(fd,監視対象のアドレスルール);
while(1){
   new_fd=accept(fd);
   if(fork() == 0){
      close(fd);
      hijack(new_fd);
      while(1){
         new_fdを使ってサーバ～クライアントのデータ通信を解析する
         write(new_fd,送信するデータ,送信先);
      }
   }
   close(new_fd);
}
```

【図２７】

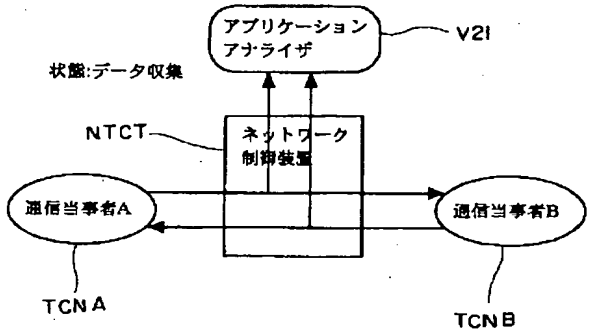


【図１９】

(A)

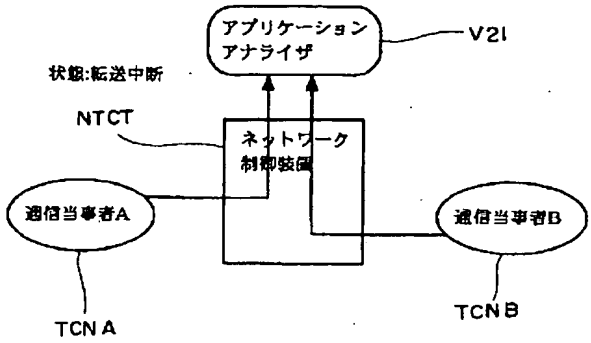


(B)

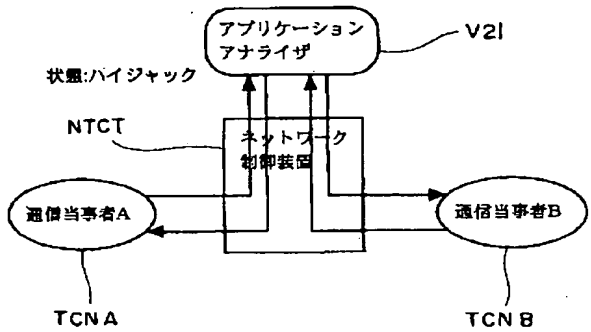


【図２０】

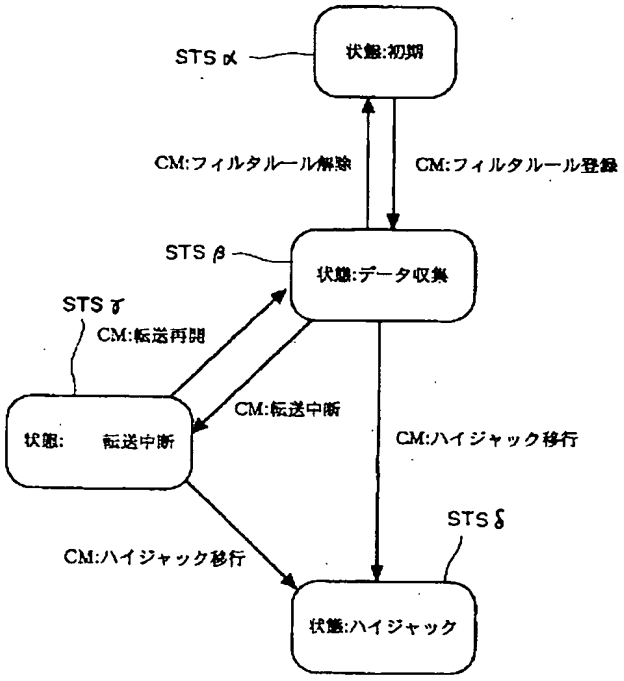
(A)



(B)



【図２１】



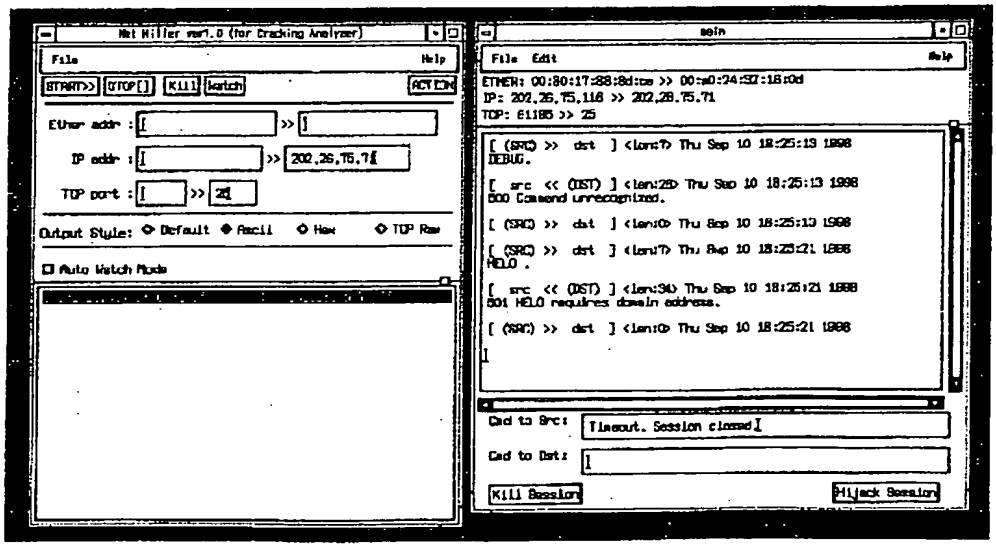
【図２４】

```
+-------------------------------------------------------+
|                        START                          |
+-------------------------------------------------------+

ETHER: 00:80:17:88:8d:ce >> 00:a0:24:32:16:0d
IP: 202.26.75.116 >> 202.26.75.71
TCP: 40508 >> 23

[ src  << (DST) ](id:4553)<len:71> Mon Aug 31 09:58:13 1998
...
BSDI BSD/OS 3.0 (netlog.nal.go.jp) (ttyp0)...
...
..*.
.....login:
[ (SRC) >>  dst  ](id:4553)<len:10> Mon Aug 31 09:58:13 1998
..*.......
[  src  << (DST) ](id:4553)<len:0> Mon Aug 31 09:58:14 1998

[ (SRC) >>  dst  ](id:4553)<len:1> Mon Aug 31 09:58:18 1998
r
[  src  << (DST) ](id:4553)<len:1> Mon Aug 31 09:58:18 1998
r
[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:18 1998

[ (SRC) >>  dst  ](id:4553)<len:1> Mon Aug 31 09:58:22 1998
o
[  src  << (DST) ](id:4553)<len:1> Mon Aug 31 09:58:22 1998
o
[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:23 1998

[ (SRC) >>  dst  ](id:4553)<len:1> Mon Aug 31 09:58:23 1998
t
[  src  << (DST) ](id:4553)<len:1> Mon Aug 31 09:58:23 1998
t
[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:23 1998

[ (SRC) >>  dst  ](id:4553)<len:1> Mon Aug 31 09:58:24 1998
.
[  src  << (DST) ](id:4553)<len:10> Mon Aug 31 09:58:24 1998
.....*....
[ (SRC) >>  dst  ](id:4553)<len:10> Mon Aug 31 09:58:24 1998
.....*....
[  src  << (DST) ](id:4553)<len:4> Mon Aug 31 09:58:24 1998
...
```

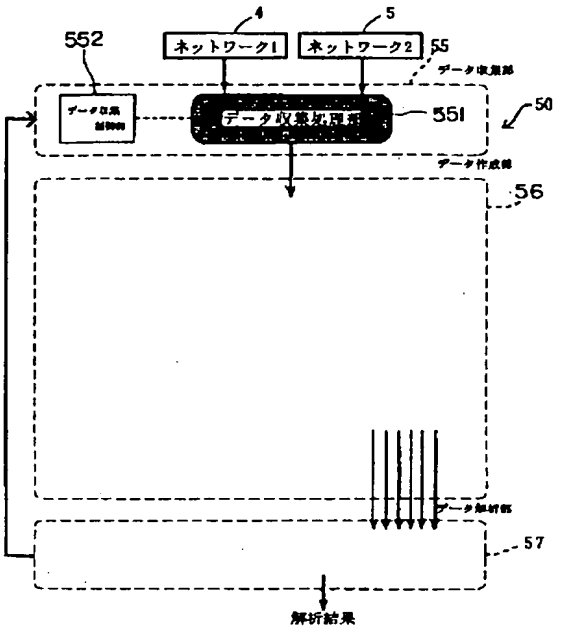
【図２５】

```
[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:24 1998

[  src  << (DST) ](id:4553)<len:12> Mon Aug 31 09:58:24 1998
...Password:
[ (SRC) >>  dst  ](id:4553)<len:3> Mon Aug 31 09:58:24 1998
...
[  src  << (DST) ](id:4553)<len:0> Mon Aug 31 09:58:24 1998

[ (SRC) >>  dst  ](id:4553)<len:7> Mon Aug 31 09:58:32 1998
root01

[  src  << (DST) ](id:4553)<len:2> Mon Aug 31 09:58:32 1998
.

[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:32 1998

[  src  << (DST) ](id:4553)<len:31> Mon Aug 31 09:58:32 1998
..*.
..login incorrect.

login:
[ (SRC) >>  dst  ](id:4553)<len:7> Mon Aug 31 09:58:32 1998
..*....
[  src  << (DST) ](id:4553)<len:0> Mon Aug 31 09:58:32 1998

[ (SRC) >>  dst  ](id:4553)<len:1> Mon Aug 31 09:58:37 1998
.
[  src  << (DST) ](id:4553)<len:4> Mon Aug 31 09:58:37 1998
...

[  src  << (DST) ](id:4553)<len:10> Mon Aug 31 09:58:37 1998
.....*....
[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:37 1998

[ (SRC) >>  dst  ](id:4553)<len:0> Mon Aug 31 09:58:37 1998

[  src  << (DST) ](id:4553)<len:0> Mon Aug 31 09:58:37 1998

+-------------------------------------------------------+
|                        END                            |
+-------------------------------------------------------+
```

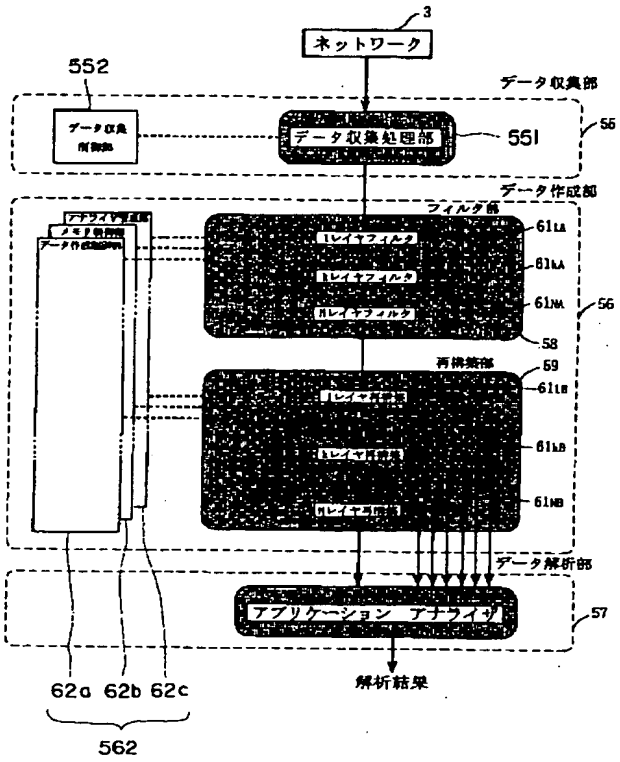
【図２６】



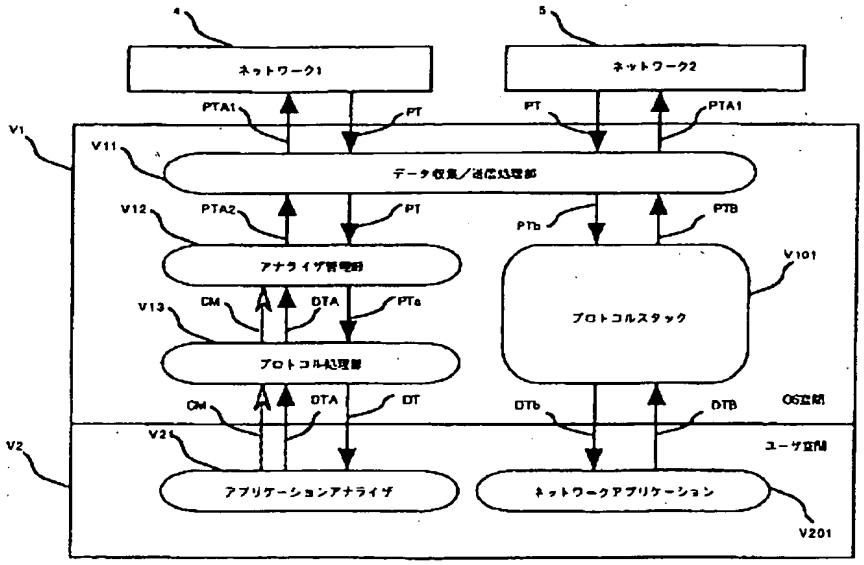
【図２８】


552
4
ネットワーク1
5
ネットワーク2
55
データ収集部
データ収集処理部
551
50
データ作成部
56
データ解析部
57
解析結果

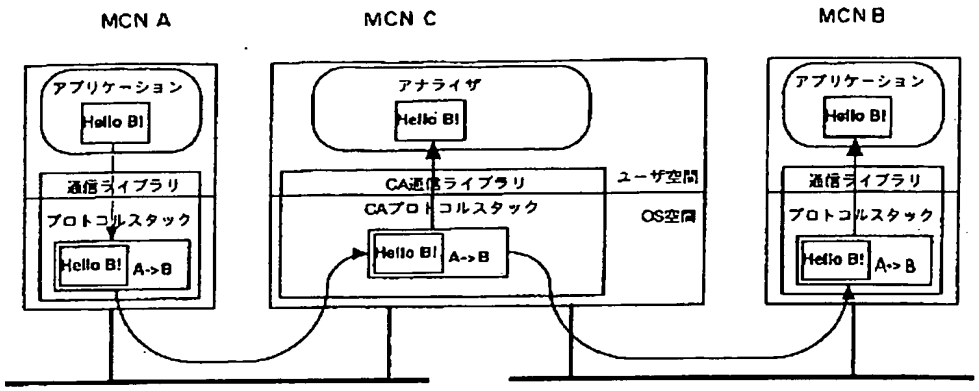
【図２９】


3
ネットワーク
552
データ収集部
データ収集処理部
551
56
データ作成部
フィルタ部
61La
61Lb
61Ma
61Mb
56
58
再構築部
59
61Ln
61Mn
データ解析部
アプリケーション アナライザ
57
解析結果
62a 62b 62c
562

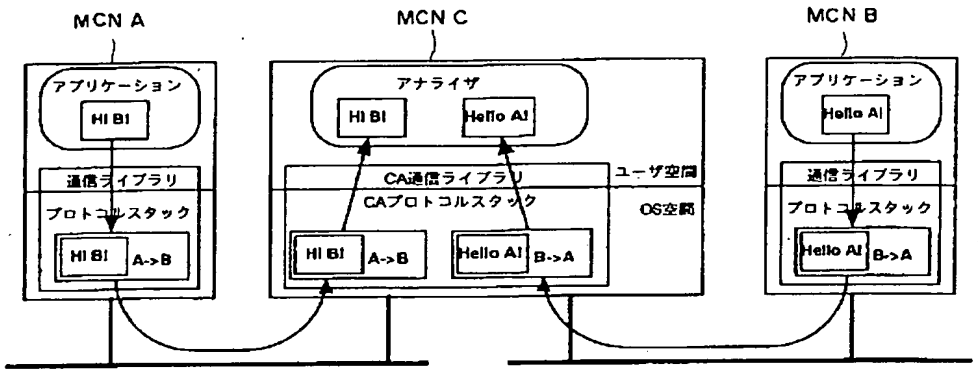
【図３０】


4
ネットワーク1
5
ネットワーク2
PTA1
PT
PT
PTA1
V1
V11
データ収集／通信処理部
V12
PTA2
PT
PTb
PTB
アナライザ管理部
V101
V13
CM
DTA
PTa
プロトコルスタック
プロトコル処理部
CM
DTA
DT
DTb
DTB
OS空間
V2
V21
ユーザ空間
アプリケーションアナライザ
ネットワークアプリケーション
V201

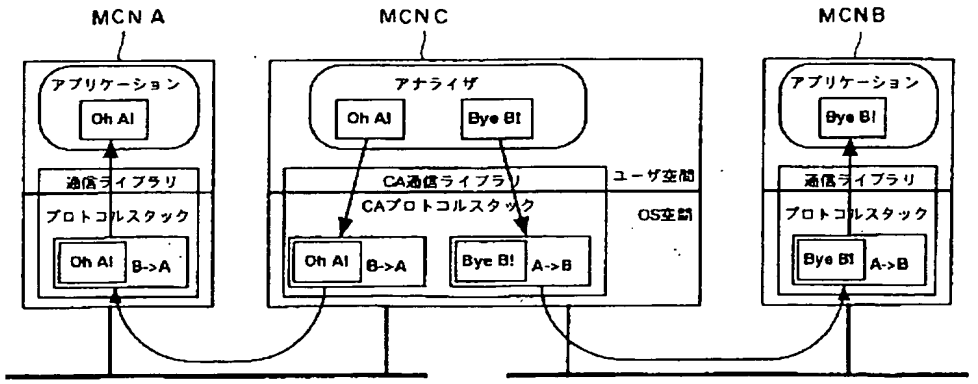
【図３１】


MCN A
MCN C
MCN B
アプリケーション
Hello B!
通信ライブラリ
プロトコルスタック
Hello B!
A->B
アナライザ
Hello B!
CA通信ライブラリ
CAプロトコルスタック
ユーザ空間
OS空間
Hello B!
A->B
アプリケーション
Hello B!
通信ライブラリ
プロトコルスタック
Hello B!
A->B

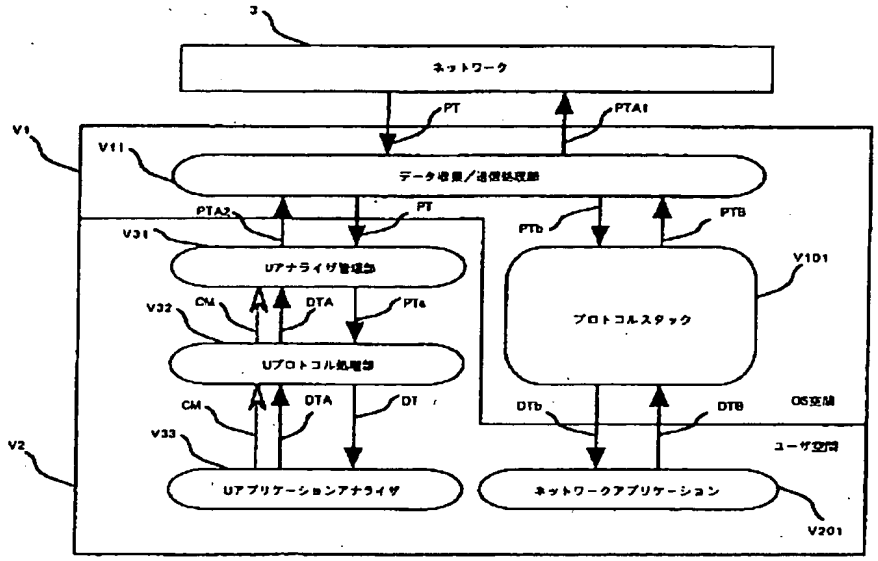
【図３２】


MCN A
MCN C
MCN B
アプリケーション
HI B!
通信ライブラリ
プロトコルスタック
HI B!
A->B
アナライザ
HI B!
Hello A!
CA通信ライブラリ
CAプロトコルスタック
ユーザ空間
OS空間
HI B!
A->B
Hello A!
B->A
アプリケーション
Hello A!
通信ライブラリ
プロトコルスタック
Hello A!
B->A

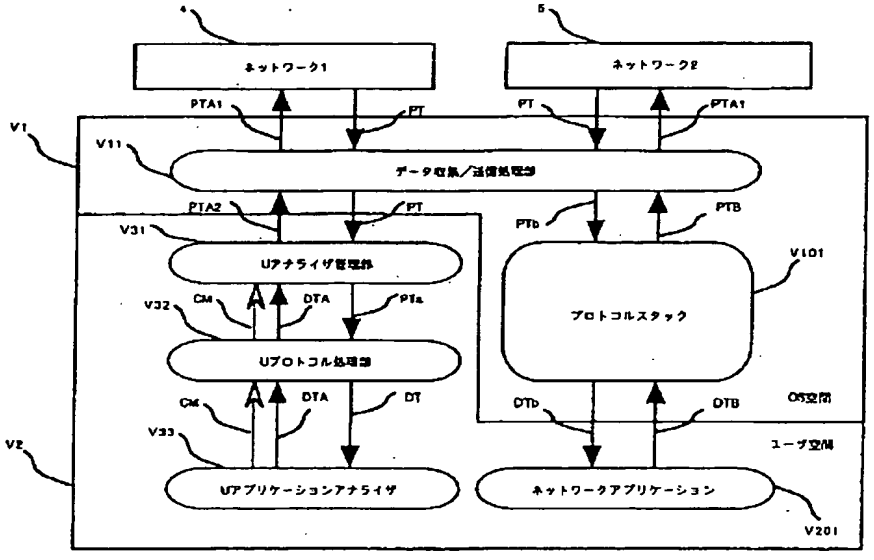
【図３３】


MCN A
MCNC
MCNB
アプリケーション
Oh A!
通信ライブラリ
プロトコルスタック
Oh A!
B->A
アナライザ
Oh A!
Bye B!
CA通信ライブラリ
CAプロトコルスタック
ユーザ空間
OS空間
Oh A!
B->A
Bye B!
A->B
アプリケーション
Bye B!
通信ライブラリ
プロトコルスタック
Bye B!
A->B

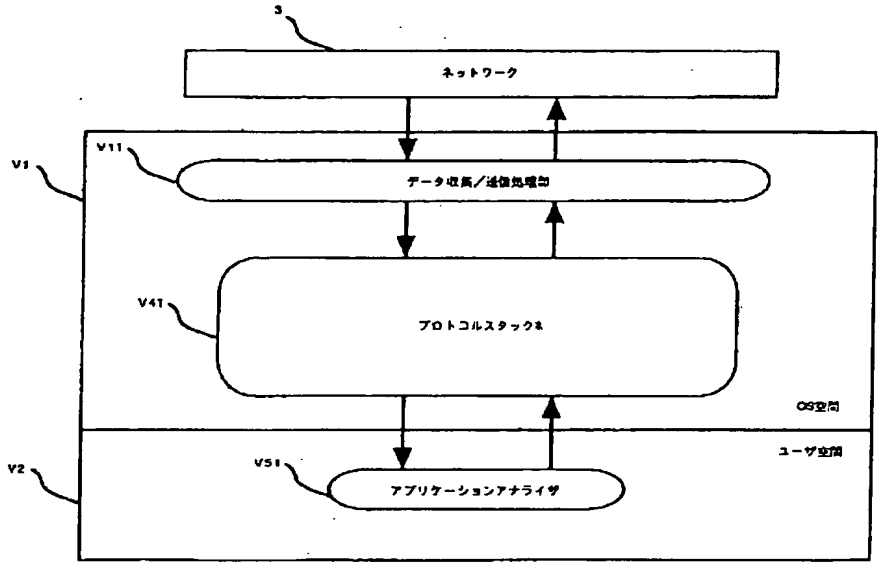
【図３４】


3
ネットワーク
PT
PTA1
V1
V11
データ収集／通信処理部
PTA2
PT
PTb
PTB
V31
Uアナライザ管理部
V101
V32
CM
DTA
PTa
プロトコルスタック
Uプロトコル処理部
CM
DTA
DT
DTb
DTB
OS空間
V33
V2
ユーザ空間
Uアプリケーションアナライザ
ネットワークアプリケーション
V201

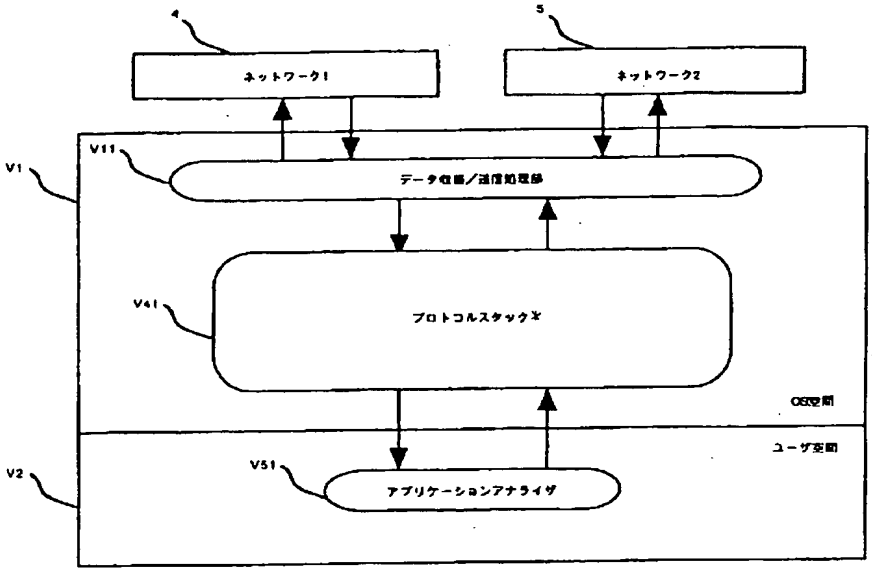
【図３５】


4
5
ネットワーク1
ネットワーク2
PTA1
PT
PT
PTA1
V1
V11
データ収集／通信処理部
PTA2
PT
PTb
PTB
V31
Uアナライザ管理部
V101
V32
CM
DTA
PTa
プロトコルスタック
Uプロトコル処理部
CM
DTA
DT
DTb
DTB
OS空間
V33
V2
ユーザ空間
Uアプリケーションアナライザ
ネットワークアプリケーション
V201

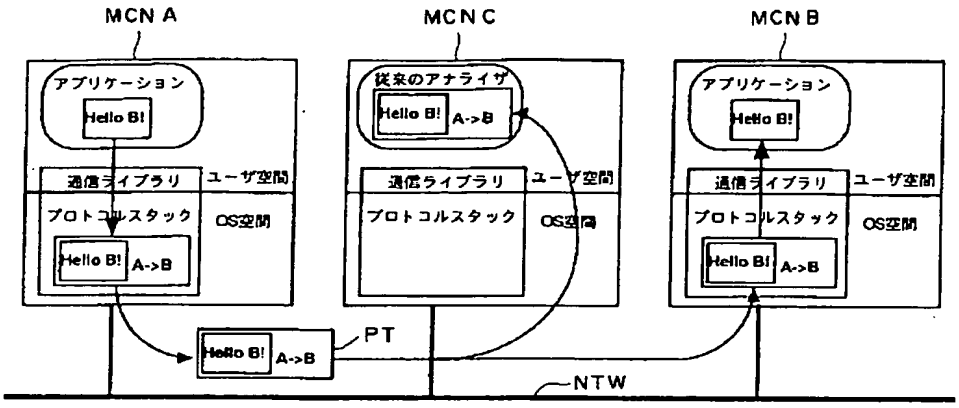
【図３６】


3
ネットワーク
V11
V1
データ収集／通信処理部
V41
プロトコルスタック#
OS空間
ユーザ空間
V2
V51
アプリケーションアナライザ

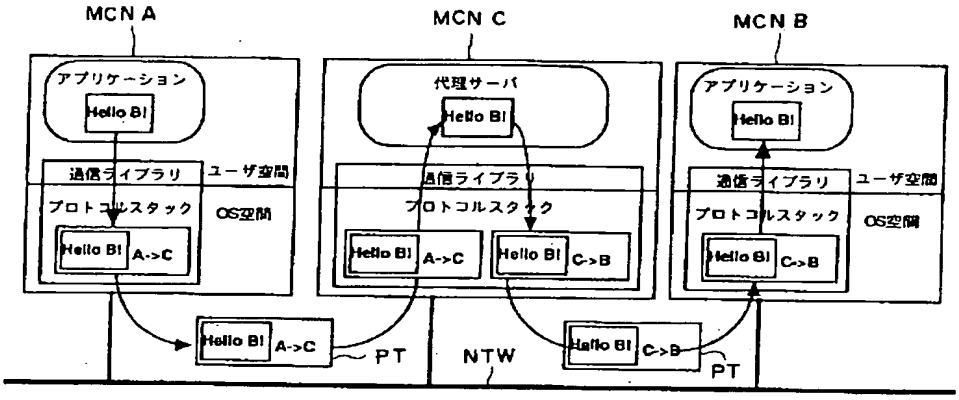
【図３７】


4
ネットワーク1
5
ネットワーク2
V11
V1
データ収集／通信処理部
V41
プロトコルスタック#
OS空間
ユーザ空間
V2
V51
アプリケーションアナライザ

【図３８】



【図３９】



フロントページの続き

(72)発明者　藤田　直行
東京都小金井市前原町４－17－28

Ｆターム(参考)　5B089 GA01 GB02 HB11 JB19 KB03
KB13 KC47 KE01 MC08
5K030 GA16 HA08 MC07